NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SECURITY VS. LIBERTY: HOW TO MEASURE PRIVACY COSTS IN DOMESTIC SURVEILLANCE PROGRAMS

by

Samuel A. Morgan

March 2014

Thesis Advisor: Erik J. Dahl
Second Reader: Robert Simeral

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
SECURITY VS. LIBERTY: HOW TO MEASURE PRIVACY COSTS IN DOMESTIC SURVEILLANCE PROGRAMS

5. FUNDING NUMBERS

6. AUTHOR(S) Samuel A. Morgan

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release;distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The June 2013 disclosure that the National Security Agency collects information on U.S. citizens revived the debate over the proper balance between national security and civil liberties. Central to the conversation is the concept of privacy. If the government is going to collect intelligence on individuals in order to defeat terrorism, then it must penetrate the veil of privacy.

The outcome of the security versus privacy debate relies on three main factors: 1) the nature of the threat; 2) the effectiveness of intelligence methods taken by the government to counter that threat; and 3) the effect those intelligence efforts have on Americans' privacy. Although imprecise and controversial, methods for measuring the threat and the effectiveness of intelligence efforts against that threat exist in various forms. It does not appear, however, that the impact of surveillance on privacy is measured in any useful way. This thesis addresses the problem of measuring privacy costs by examining the following questions: What elements of government surveillance programs and privacy expectations must be taken into account? What level of domestic surveillance is acceptable to the American public? And finally, how can we measure the cost of privacy to better inform the security versus liberty debate?

14. SUBJECT TERMS Liberty, Privacy, Domestic Surveillance, National Security Agency, Total Information Assurance, Church Committee, Telephone Metadata, FISC.

15. NUMBER OF PAGES 105

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SECURITY VS. LIBERTY: HOW TO MEASURE PRIVACY COSTS IN DOMESTIC SURVEILLANCE PROGRAMS

Samuel A. Morgan
Lieutenant, United States Navy
B.A., Gonzaga University, 2003
M.A., St. John's University, 2009

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2014**

Author: Samuel A. Morgan

Approved by: Erik J. Dahl
Thesis Advisor

Robert Simeral
Second Reader

Mohammed M. Hafez, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The June 2013 disclosure that the National Security Agency collects information on U.S. citizens revived the debate over the proper balance between national security and civil liberties. Central to the conversation is the concept of privacy. If the government is going to collect intelligence on individuals in order to defeat terrorism, then it must penetrate the veil of privacy.

The outcome of the security versus privacy debate relies on three main factors: 1) the nature of the threat; 2) the effectiveness of intelligence methods taken by the government to counter that threat; and 3) the effect those intelligence efforts have on Americans' privacy. Although imprecise and controversial, methods for measuring the threat and the effectiveness of intelligence efforts against that threat exist in various forms. It does not appear, however, that the impact of surveillance on privacy is measured in any useful way. This thesis addresses the problem of measuring privacy costs by examining the following questions: What elements of government surveillance programs and privacy expectations must be taken into account? What level of domestic surveillance is acceptable to the American public? And finally, how can we measure the cost of privacy to better inform the security versus liberty debate?

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ARM	Activity, Recognition and Monitoring
BR	business record
COINTELPRO	Counter Intelligence Program
COMINFIL	Communist Infiltration
COMSAB	Communist Sabotage
DARPA	Defense Advanced Research Agency
DETCOM	Detention of Communists
DOD	Department of Defense
DOJ	Department of Justice
EELD	Evidence Extraction and Link Discovery
FISA	Foreign Intelligence Surveillance Act
FISC	FISA Court
HPSCI	House Permanent Select Committee on Intelligence
HumanID	Human Identification at a Distance
IC	intelligence community
IG	Inspector General
IMEI	international mobile station equipment identity
IMSI	international mobile subscriber identity
MInDet	MisInformation Detection
MIT	Massachusetts Institute of Technology
NCTC	National Counterterrorism Center
NGFR	Next-Generation Face Recognition
NSA	National Security Agency
NSD	National Security Division
NSL	National Security Letter
ODNI	Office of the Director of National Intelligence
OGC	Office of General Council
PIA	privacy impact assessment
PPD-28	Presidential Policy Directive-28
RAS	reasonable, articulable suspicion

SIGINT	signals intelligence
SSCI	Senate Select Committee on Intelligence
SSNA	Scalable Social Network Analysis
TIA	Total Information Awareness
TIDE	Terrorist Identities Datamart Environment

ACKNOWLEDGMENTS

I would like to thank Mr. Robert Simeral for his feedback and guidance as my second reader. I would also like to thank my advisor, Professor Erik Dahl. I came to you with a complex way of approaching a broad, evolving problem, and you still agreed to work with me on this project. Thank you for your trust, patience, and mentorship throughout this process. Finally, I would like to thank my wife, Elizabeth. I cannot imagine anyone being more understanding and supportive than you have been throughout this process. You lovingly accepted that the long hours this thesis required meant that I had less time to spend with you. ΕΥΧΑΡΙΣΤΟΥΜΕ, ΑΓΑΠΗ ΜΟΥ.

THIS PAGE INTENTIONALLY LEFT BLANK

I. SECURITY VERSUS LIBERTY

A. MAJOR RESEARCH QUESTION

The June 2013 disclosure that the National Security Agency (NSA) collects information on U.S. citizens revived the debate over the proper balance between national security and civil liberties. The current iteration of the dispute focuses on the use of domestic surveillance tools to support the state's interest in protecting against terrorism versus society's interest in civil liberties. Central to the conversation is the concept of privacy because it is "the one aspect of liberty that inhibits the government's acquisition of information."[1] Thus, if the government is going to collect intelligence on individuals in order to defeat terrorism, then it must penetrate the veil of privacy.

The outcome of the security-versus-privacy debate relies on three main factors: 1) the nature of the threat; 2) the effectiveness of intelligence methods taken by the government to counter that threat; and 3) the effect those intelligence efforts have on Americans' privacy. If the purpose of the debate is to reconcile the tensions between competing security and liberty interests, the fundamental question is how do we measure each component in order to balance the scale? What values are we to give to threat, intelligence, and privacy in order to correctly convert the gain on one side with a proportionate, acceptable loss on the other? Although imprecise and controversial, methods for measuring the threat and the effectiveness of intelligence efforts against that threat exist in various forms. It does not appear, however, that the impact of surveillance on privacy is measured in any useful way.

This thesis addresses the problem of measuring privacy costs by examining the following questions: What elements of government surveillance programs and privacy expectations must be taken into account? What level of domestic surveillance is acceptable to the American public? And finally, how can we measure the cost of privacy to better inform the security versus liberty debate?

---

[1] Richard Betts, *Enemies of Intelligence: Knowledge is Power in American National Security* (New York: Columbia University Press, 2007): 163, quoted in Gregory F. Treverton, *Intelligence for an Age of Terror* (Cambridge: Cambridge University, 2009), 242.

B. LITERATURE REVIEW

Discussions about the tensions between security and liberty usually come down to three core arguments. The primacy of security position argues that the threat is high, and thus security trumps concerns over civil liberties. Conversely, the defense of liberty argument tends to undervalue the threat while making civil liberties absolute and non-sacrificial. Between these two poles rests a more practical but flawed approach, referred to here as the balancing act, which argues for a balance between the competing security and liberty interests.

Central to the primacy of security position is the argument that without security, there is no freedom. Therefore, individual rights are submissive to overall security concerns.[2] Proponents argue that the historical record favors this side of the debate. They are quick to point out that during the Civil War, World War I, World War II, and the Cold War, up until the post-Vietnam era, the state routinely infringed on civil liberties in order to protect the country from threats.[3] Because security is a prerequisite for freedom, the logic continues, the state is free to do anything necessary.[4] In the extreme form, Richard Posner goes so far as to argue the government has the moral duty "to violate legal, including constitutional, rights when necessary to avoid catastrophic harm to the nation."[5] This position also holds that the Constitution does not specifically provide a right to privacy anyway, and, even if it did, the status of civil liberties return once the threat is defeated.[6] A fundamental challenge to the primacy of security position is that

---

[2] Alan F. Westin, "How the Public Sees the Security-versus-Liberty Debate," in *Protecting What Matters: Technology, Security, and Liberty since 9/11*, ed. Clayton Northouse (Washington, DC: Brookings, 2005), 19; Richard A. Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (New York: Oxford University, 2006), 4; Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven: Yale University, 2011), 209.

[3] Jerel A. Rosati, "At Odds with One Another: The Tension between Civil Liberties and National Security in Twentieth-Century America," in *American National Security and Civil Liberties in an Era of Terrorism*, ed. David. B. Cohen and John W. Wells (New York: Palgrave Macmillan, 2004), 11–12; Solove, *Nothing to Hide*, 55–56, 59.

[4] Julian Richards, "Intelligence Dilemma? Contemporary Counter-terrorism in a Liberal Democracy," *Intelligence and National Security* 27, no. 5 (2012): 764.

[5] Posner, *Not a Suicide Pact*, 14.

[6] Ibid., 127; Solove, *Nothing to Hide*, 60–61.

security is more than physical threats; defending democracy also "requires the defense of democracy's ideals."[7]

The defense of liberty school directly challenges the logic of the security first position through five main counterarguments. First, the historical record demonstrates contractions of liberties during war in what is otherwise an expansion of civil liberties over time.[8] Second, justifications are usually based on a preoccupation with internal threats during war, with questionable validity and only the hope, not assurance, that liberties will return after the threat ceases.[9] Third, there is no correlation between decreasing liberty and increased security.[10] Authors such as Bruce Schneier argue, "bad security can be worse than no security" because of its negative effects on liberties without any positive gain for security.[11] Fourth, if the Constitution is not a suicide pact, "neither is war a blank check"[12]—meaning there must be limits to state powers even in the face of a persistent, deadly threat. Fifth, even with multiple attacks on the scale of 9/11, terrorism is not an existential threat, while eroding liberties is.[13] Therefore, efforts that weaken the Constitution are a bigger threat to the state than terrorism.[14] The basic conclusion of this school is that the defense of liberty supersedes all other considerations; subjecting rights to security interests makes the cure for terrorism worse than the infirmity.

At the core of the defense of liberty school of thought is the simple but profound premise that civil liberties are absolute, unalienable rights that cannot be broken no matter what the threat is.[15] Derived from this underlying position is the conclusion that

---

[7] Brian Jenkins, *Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves* (Santa Monica, CA: RAND, 2006): 176, quoted in Treverton, *Intelligence for Age of Terror*, 261.

[8] Rosati, "At Odds with One Another," 11, 23–24.

[9] Ibid.; Solove, *Nothing to Hide*, 60–61.

[10] Solove, *Nothing to Hide*, 34.

[11] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York: Copernicus, 2003), 10,14.

[12] Treverton, *Intelligence for Age of Terror*, 253.

[13] Ibid., 261.

[14] Westin, "How Public Sees Security-versus-Liberty Debate," 19.

[15] David B. Cohen and John W. Wells, *American National Security and Civil Liberties in an Era of Terrorism*, 1.

intelligence collection that infringes on liberty is unethical, and therefore must be avoided even if it is effective against a threat.[16] This, however, is an unsustainable application of security concerns. Just as national security means very little if it destroys liberty, so, too, is liberty meaningless without physical security. Failing to recognize this will turn "give me liberty, or give me death"[17] into a near certainty of having both liberty and death.

The balancing act, the third approach, criticizes the first two for discrediting the debate by applying extreme arguments.[18] At first look, it appeared as if the false-choice argument and the balanced approach were two separate positions. As it turns out, the complementary nature of the two cannot be avoided: the false choice reflects this school's underlying views, while the balancing act is how to resolve security and liberty interests. The core elements of the false-choice position are that both liberty and security are important, the two do not necessarily contradict each other, and the state can and must protect both.[19] With these ground rules set, the challenge becomes how to balance security and liberty interests against a threat that brings the battle-space to the domestic front.[20]

---

16 Richards, "Intelligence Dilemma?" 764.

17 Patrick Henry, "A Chronology of U.S. Historical Documents: Give Me Liberty or Give Me Death," University of Oklahoma, accessed September 16, 2013, http://www.law.ou.edu/ushistory/henry.shtml.

18 Treverton, *Intelligence for Age of Terror*, 252.

19 National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: Government Printing Office, 2004), 395; Bruce Berkowitz, "Policies and Procedures for Protecting Security and Liberty," in *Protecting What Matters: Technology, Security, and Liberty since 9/11*, 83; Gilman Louie and Gayle von Eckartsberg, "Security and Liberty: How Technology Can Bridge the Divide," in *Protecting What Matters: Technology, Security, and Liberty since 9/11*, 63,72; Solove, *Nothing to Hide*, 2,3 4–35,210; Cohen and Wells, *American National Security and Civil Liberties*, 1; Loch K. Johnson and James J. Wirtz, *Intelligence and National Security: The Secret World of Spies*, ed. Loch K. Johnson and James J. Wirtz, 2nd ed. (New York: Oxford University, 2008), 344–45.

20 Berkowitz, "Policies and Procedures for Protecting Security and Liberty," 74–75, 77.

The balanced approach is a process that applies a tradeoff or weighted comparison of each side's interests that produces a desirable outcome.[21] Its process relies on the threat and effectiveness of an intelligence tool to measure the national security interests and the harm to privacy to determine the civil liberty costs. That there is a relationship between threat, effectiveness, and privacy is widely recognized. The concept of a desirable balance, however, is drastically skewed because of incomplete mechanisms for weighing each side, which creates the ambiguity that permits biases of security overruling liberty or vice versa.[22] One of the main reasons for the problems in the balanced approach is the lack of methods for measuring privacy costs.

C. IMPORTANCE

Balancing national security interests and civil liberties has long been a concern in the United States.[23] The notion of a balance or tradeoff between the two sides, however, is inaccurate. While there are ways to measure the threat level as well as the effectiveness of a particular intelligence method, there is a noticeably absent value for the privacy costs against which those are to be weighed. For example, one could attempt to measure the terrorist threat by arguing that statistically, an American has a 1 in 3.5 million chance of dying in a terrorist attack every year.[24] Experts such as John Mueller contend this measurement indicates that terrorism presents less of a threat than many other concerns in society. Alternatively, an argument could be made that between 9/11 and September 2012, there was an average of one terrorist attack disrupted every two and a half months

---

[21] Cohen and Wells, *American National Security and Civil Liberties*, viii; Clayton Northouse, "Providing Security and Protecting Liberty," in *Protecting What Matters: Technology, Security, and Liberty since 9/11*, 4,8–9; Schneier, *Beyond Fear*, 3; Richards, "Intelligence Dilemma?" 763–64; Solove, *Nothing to Hide*, 207; Treverton, *Intelligence for Age of Terror*, 241; Rosati, "At Odds with One Another," 24–25; Garrett Hatch, *Privacy and Civil Liberties Oversight Board: New Independent Agency Status*, CRS Report RL34385 (Washington, DC: Library of Congress. Congressional Research Service, August 27, 2012), 1, 6; Berkowitz, "Policies and Procedures for Protecting Security and Liberty," 83.

[22] Westin claims that all positions are about either security or liberty first; all other positions are nuances of one of the two; Westin, "How Public Sees Security-versus-Liberty Debate," 19.

[23] Rosati, "At Odds with One Another," 11–12; Susan J. Tabrizi, "At What Price? Security, Civil Liberties, and Public Opinion in the Age of Terrorism," in *American National Security and Civil Liberties in an Era of Terrorism*, 185–86.

[24] John Mueller and Mark G. Steward, "Hardly Existential: Thinking Rationally About Terrorism," *Foreign Affairs*, April 2, 2010, http://www.foreignaffairs.com/articles/66186/john-mueller-and-mark-g-stewart/hardly-existential.

within the United States.[25] This supports a different measurement—one of a persistent and serious threat. Determining which of these approaches is the most appropriate is beyond the scope of this thesis, but the point is that we at least have ways of measuring the threat.

Measuring effectiveness is also possible, such as through demonstrating a correlation or causation between an intelligence tool and the disruption of terrorist activities. NSA Director General Keith Alexander and FBI Deputy Director Sean Joyce justified the necessity of the NSA's domestic surveillance tools by applying this rationale during their testimony to the House Permanent Select Committee on Intelligence (HPSCI). Both Alexander and Joyce credited the surveillance programs with preventing more than 50 terrorist events, including 10 targeting the United States and a specific threat against the New York Stock Exchange.[26] Others, however, claim the NSA tools hardly contributed anything to the prevention of those plots and to no more than 7.5 percent of all disrupted terrorist activities within the United States since 9/11.[27] Irrespective of the value, there are methods by which we can measure the effectiveness of various domestic surveillance tools.

On the other side of the scale, however, there is no generally accepted measurement for the civil-liberty costs incurred by domestic intelligence programs. This makes it impossible to determine where the balance between security and liberty lies and whether it needs adjusted. The political response to the 2013 disclosures of domestic surveillance programs demonstrates the negative effects of an incomplete balancing

---

[25] Jessica Zuckerman, "Fifty-Third Terror Plot Foiled Since 9/11: Bombing Targets U.S. Financial Hub," Heritage Foundation, Issue Brief 3758 (2012), http://www.heritage.org/research/reports/2012/10/terror-plot-foiled-in-new-york-bombing-targets-us-financial-hub.

[26] Patricia Zengerle and Tabassum Zakaria, "NSA Head, Lawmakers Defend Surveillance Programs," *Reuters*, June, 18, 2013, http://www.reuters.com/article/2013/06/18/us-usa-security-idUSBRE95H15O20130618; Patricia Zengerle, "FBI Official Says NSA Programs Helped Foil NYSE Bombing Plot," *Reuters*, June 18, 2013, http://www.reuters.com/article/2013/06/18/us-usa-security-nyse-idUSBRE95H0QT20130618.

[27] Peter Bergen et. al., "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New America Foundation, January 2014, 4–5, http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0_0.pdf.

framework. Arguments against the NSA's activities by civil-liberties advocates progressed under the assumption that intelligence surveillance has crept too far into civil liberties, and therefore the government must reform its surveillance programs and processes.[28] Advocates for the programs argued that the NSA surveillance efforts actually impose little, if any, harm to civil liberties. Neither side made a convincing case because neither side could provide specific assessments regarding privacy costs. Consequently, as more revelations about government surveillance capabilities emerged, the pressure grew and tipped the balance in favor of privacy interests. In January 2014, intelligence reforms were announced by the White House. In essence, our inability to measure the civil-liberty side of the scale has inclined the nation to alter current practices based on a perception that there is an unacceptable level of encroachment simply because surveillance occurs.

D. PROBLEMS AND HYPOTHESES

A fundamental problem this thesis must address is how to determine which factors are relevant to measuring privacy costs. Comparing Cold War-era domestic intelligence violations with those of modern programs could provide valuable insight into what the key variables are. For example, out of the one million Americans the FBI kept records on between 1960 and 1974, it investigated 500,000 of them it suspected were subversives without convicting a single person.[29] Americans rejected these FBI practices as unacceptable. Similarly, privacy concerns led Congress to defund the Pentagon's Total Information Awareness (TIA) program in 2003, which would have collated all information about a person from government records as well as every private transaction a person conducts.[30] These two cases serve as examples of domestic intelligence that

[28] Kristina Peterson and Siobhan Hughes, "Disclosures on NSA's Surveillance Embolden Its Critics in Congress," *Wall Street Journal*, August 24, 2013, http://online.wsj.com/article/SB10001424127887323665504579029362415300556.html.

[29] George Santayana, "History Repeated: The Dangers of Domestic Spying by Federal Law Enforcement," American Civil Liberties Union, accessed September 12, 2013, https://www.aclu.org/sites/default/files/images/asset_upload_file893_29902.pdf.

[30] Northouse, "Providing Security and Protecting Liberty," 3–4.

Americans viewed as too costly to their privacy; the reasons why could inform what to look for in other programs.

Another problem is that societal developments challenge traditional interpretations of privacy. This is extremely important to the discussion because without a valid privacy interest, there are grounds to argue that there is no privacy cost. Moreover, a measurement of privacy costs would be incomplete without integrating all areas of legitimate privacy interests. It is therefore necessary to establish what is a valid privacy interest. In support of this end, it might be useful to explore the amount of personal information Americans freely provide, to whom, how often, and what private details it reveals. For example, major telecommunications companies in the United States collect data on the location of a person's phone, incoming and outgoing calls and messages, and Internet use and, depending on the company, store the information from a period of one year to indefinitely.[31] Is society more willing to permit the access and use of this information to a company in order to receive a service than to allow the government access and use of the same information in order to provide security? Analyzing the role of technology in today's society compared with the intent of Fourth Amendment protections could help establish a standard of American privacy against which to assess the extent of domestic surveillance tools.

This thesis hypothesizes that two primary issues translate into privacy costs. First is the expectation Americans have for government behavior, such as abusive use of surveillance powers or how well the government safeguards personal information in order to minimize privacy concerns. Second is the expectation Americans have for privacy, at both the individual and societal level.

E. METHODS AND SOURCES

The first task will be to determine what expectations Americans have for government behavior by conducting historical comparison and analysis of domestic

[31] David Kravets, "Which Telecoms Store Your Data the Longest? Secret Memo Tells All," *Wired*, September 28, 2011, http://www.wired.com/threatlevel/2011/09/cellular-customer-data/; "Fact Sheet 2b: Privacy in the Age of the Smartphone," Privacy Rights Clearinghouse, accessed September 13, 2013, https://www.privacyrights.org/fs/fs2b-cellprivacy.htm.

surveillances programs that society rejected as unacceptable. This section will primarily rely on Congressional hearings and reports, Inspector General (IG) reports, and information the government released about surveillance programs. The result of this process will be to capture the lessons learned from failed domestic surveillance experiences, identify what the major factors are for scrutinizing privacy concerns and safeguards, and then determine how these fit into a model for measuring privacy costs of other domestic intelligence programs.

The second task will be to establish what expectations Americans have for their privacy. To reach this conclusion the thesis will rely on the comparison between two competing indicators: the historical standards for the expectation of privacy and the modernization of society. Sources for this section will be Supreme Court case law, statistics about American's use of technology, and examples of how the nature of information is becoming more personal. This section will conclude with new standards for what constitute a subjective and reasonable expectation of privacy, which will be applied to the model for measuring privacy costs.

Once the expectations for government behavior and privacy are established, the lessons from both will be turned into a model for measuring privacy costs. This model will then be applied to a current intelligence program, which will rely on declassified government documents, public statements made by politicians and intelligence leaders, and new intelligence policy directives.

F. OVERVIEW

In Chapter II, the thesis turns to the expectations Americans have for government behavior in domestic intelligence by examining the experiences of Cold War-era and TIA programs. Chapter III will address the expectations Americans have for privacy. Chapter IV will provide a model for measuring privacy costs based on the lessons and conclusions of Chapter II and Chapter III. In Chapter V, the NSA's bulk metadata collection program under Section 215 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Patriot Act) will be tested against this model. It will also review 2014 intelligence reforms to evaluate what effect, if

any, these reforms had on the privacy costs associated with the NSA program. Chapter VI will conclude with suggestions for ways forward, to include which programs the United States might need to reevaluate in order to strike an accurate balance with the security interest of the state.

II. EXPECTATIONS FOR GOVERNMENT BEHAVIOR

Privacy violations come in the form of government activities against its citizens. It is therefore instructive to review government programs that society rejected as having too high of privacy costs. These discontinued surveillance programs expose the core elements that society deems unacceptable government behavior because of the associated infringements on privacy. What follows are analyses of CIA, FBI, and NSA surveillance activities from the 1940s through 1970s, and the Total Information Awareness initiative of the early 2000s. The purpose of this chapter is to discuss the capabilities and privacy implications of the various programs, which will inform the Chapter IV discussion on how to measure privacy costs.

A. COLD WAR PROGRAMS

On January 27, 1975, the U.S. Senate established a special committee to investigate public allegations of widespread misconduct by the intelligence community (IC).[32] The mandate of the Church Committee was broad and included the following:

- determine what activities the intelligence agencies conducted,
- what activities these agencies should conduct,
- whether those activities conformed to the law and Constitution,
- if the existing laws were inadequate to protect the rights of citizens, and
- how to improve oversight of the different intelligence agencies.[33]

In order to accomplish its objectives, the Committee focused on the authorities, organization, and activities of the CIA, NSA, FBI, the intelligence components of the Department of Defense, and the National Security Council.[34] By the time it concluded in May 1976, the Church Committee had detailed the intelligence agencies' expansive

[32] Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Intelligence Activities and the Rights of Americans: Final Report*, Book II, S. Rep. No. 94-755, at v (1976); "Church Committee Created," U.S. Senate, accessed March 2, 2014, http://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm.

[33] S. Rep. No. 94-755, at vi (1976).

[34] Ibid., at vii.

violations of constitutionally protected rights. These CIA, NSA, and FBI programs stand as examples of unendurable infringements on privacy.

1. Capabilities

The apparent partition between the intelligence programs and agencies during the 1940s and 1970s is deceiving. While the CIA, NSA, and FBI oversaw their own activities, they also shared intelligence with other offices in their organizations and with each other. Frequently the intelligence sharing went beyond what was legally permissible and extended into coordinated domestic surveillance. In order to understand the full scope of the privacy infringements, it is necessary to evaluate each program individually while also considering the capabilities it provided to the overall domestic intelligence apparatus.

a. CIA: CHAOS

Starting around August 1967 and ending in March 1974, the CHAOS program was an intelligence operation ran by the CIA to determine if the Soviets, Chinese Communists, and Cubans were exploiting domestic protests within the United States as a means to conduct espionage and subversion.[35] The program originally focused on the potential foreign communist control of the anti-Vietnam War and the Black Power movements. Despite evidence indicating the absence of any significant foreign influence in these movements, CHAOS broadened in scope.[36] One of the main reasons for expanding the program, according to former Director of the CIA Richard Helms, was that in order for the CIA to accurately conclude there was no significant foreign influence, it had to prove the negative: it needed to investigate all the anti-war protestors and their contacts to ensure no association existed between them and foreign powers.[37] This defective rationale, however, was not the only reason why the CHAOS program broadened to other domestic protestors. The White House initiated the program through persistent requests to the CIA and then was skeptical of the results, consequently creating

[35] Ibid., at 100.

[36] Ibid., at 96.

[37] Ibid., at 101–02.

pressure to expand its scope.[38] In addition, the FBI submitted intelligence requirements to CHAOS for its own questionable domestic surveillance purposes, which also contributed to stretching the limits of the program's reach. The FBI started submitting names of U.S. citizens to the CIA for monitoring in 1970. Its sole justification for conducting surveillance on these people was an accusation that they engaged in domestic protests and violence.[39]

b. CIA: Mail Opening Program

Several CIA programs opened mail transiting through, to, or from the United States between 1953 and 1973.[40] The purpose was to discover Soviet Union intelligence efforts within the United States. An Inspector General (IG) report provided to the Church Committee during the hearings explained that from its office at the mail processing center at LaGuardia Airport in New York City, the CIA screened and photographed a high volume of letters, from which it selected a smaller number to steam open, copy, reseal, and place back into the mail system. Much like CHAOS, these mail opening programs broadened beyond the original purpose. Starting in 1969, the FBI submitted names of domestic political radicals and black militants for the CIA to include in its mail opening programs. By 1972, the FBI's request list expanded to include protest and peace organizations, such as the People's Coalition for Peace and Justice, the National Peace Action Committee, and the Women's Strike for Peace as well as subversive groups such as the Black Panthers, White Panthers, Black Nationalists and Liberation Groups, Students for a Democratic Society, Resist, and Revolutionary Union.[41]

[38] Ibid., at 100–101.

[39] Ibid., at 100.

[40] The FBI also had a mail-opening program but terminated it in 1966, at which point it started submitting requirements to, and receiving the benefits from, the CIA programs. Ibid., at 12, 31, 59,107.

[41] Ibid., 6,58,107–08; *Intelligence Activities: Hearing on Mail Opening, Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. (October 21–24, 1975), 176.

c. NSA: MINARET

In 1962, the NSA started collecting signals intelligence (SIGINT) on American citizens, which the government then used for domestic law enforcement purposes.[42] That program was MINARET. It was originally limited to people traveling to Cuba, but after the Warren Commission's report on the assassination of President Kennedy the Secret Service asked the NSA to monitor communications of people who were potential threats to the president.[43] Ever since this initial request the MINARET watch list primarily focused on Americans.[44] Expanding the program, however, involved more than the NSA and Secret Service. Throughout the 1960s, the MINARET watch list grew in response to FBI requests to include people suspected of narcotics related activity and domestic terrorism.[45] Not until 1973, in the immediate aftermath of the congressional hearings on Watergate, did the attorney general shutdown the MINARET program.[46]

d. NSA: SHAMROCK

From 1947 until 1975, at least three international cable companies provided the NSA with millions of private cables sent by Americans.[47] The program expanded to include essentially all the cables to or from the United States sent or received by the three major communications companies.[48] Couriers from these companies routinely transported the messages to NSA, who would then select cables for additional analysis and destroy the rest.[49] The broadening of SHAMROCK, however, was more than an increase in collection; it also reflected a breakdown of the rules in place that prohibited domestic collection by the NSA.

---

[42] Thomas R. Johnson, *Book III: Retrenchment and Reform, 1972-1980*, vol. 5, *NSA Period: 1952-Present* of a series on American Cryptography during the Cold War, 1945-1989 (National Security Agency, 1998), 84.

[43] Ibid., 84.

[44] Ibid., 84.

[45] Ibid., 85.

[46] Ibid., 86.

[47] S. Rep. No. 94-755, at 6, 12, 104 (1976).

[48] Ibid., at 104.

[49] Johnson, *Retrenchment and Reform*, 84.

e. FBI: Counterintelligence Program

The FBI's Counterintelligence Program (COINTELPRO) was designed to disrupt groups and neutralize individuals that it designated as threats to domestic security. The program originally targeted the Communist Party, U.S.A., but its focus gradually shifted toward domestic dissenters. Under COINTELPRO, the FBI collected and disseminated excessive information on people it labeled as rabble rousers, agitators, key activists, and key black extremists and then used covert action to disrupt or neutralize their influence. For example, the FBI anonymously attacked the political beliefs of Americans as a means of provoking their employer to fire them. In deliberate attempts to destroy marriages, the FBI mailed anonymous letters to the spouses of the people it was trying to neutralize. In some cases, the FBI prompted the IRS to investigate Americans as a form of harassment and to delegitimize protest leaders. Finally, targets of COINTELPRO would be physically attacked by or expelled from their group as a direct result of the FBI falsely and anonymously labeling them as government informants.[50]

f. FBI: Communist Infiltration

Similar to COINTELPRO and CHAOS, the Communist Infiltration (COMINFIL) program originally focused on communist influence of domestic activists. The Church Committee found that the FBI exaggerated the extent of domestic communist influence by foreign powers. Consequently, COMINFIL expanded into the FBI's broadest intelligence collection program. It collected a wide range of information on political, legislative, and cultural activities, youth, women's, farmers', and veterans' matters, and a person's religion and education. In effect, the COMINFIL program provided intelligence on a wide range of groups that did not have any significant connections to communists.[51]

g. FBI: Watch Lists

A key contributor to domestic intelligence abuses was the FBI's use of watch lists. The FBI's priority arrest list, known as DETCOM, contained the names of key

[50] S. Rep. No. 94-755, at 10,63,69,89 (1976).

[51] Ibid., at 48,68.

figure and functionaries of the Communist Party.[52] Similarly, the Communist Sabotage (COMSAB) list contained names of potential communist saboteurs.[53] There was also the Communist Index, which although its name implied a focus on key communists within the United States was actually much broader. The Communist Index contained people of interest to internal security irrespective of any communist connections.[54] Another important list maintained by the FBI was the Rabble Rouser Index. According to the FBI's definition, a rabble-rouser was "a person who tries to arouse people to violent action by appealing to their emotions, prejudices, et cetera."[55] In 1967, the Rabble Rouser definition expanded to include "persons with a 'propensity for fomenting' any disorders affecting the 'internal security'" of the United States.[56] The FBI renamed it the Agitator Index in 1968 and applied an even lower standard for what constituted an agitator, consequently deflating the list's value.[57]

A new initiative replaced the Agitator Index: it was known as the Key Activist program.[58] Key activists, as defined by the FBI, were: "individuals in the Students for Democratic Society and the anti-Vietnam war groups [who] are extremely active and most vocal in their statements denouncing the United States and calling for civil disobedience and other forms of unlawful and disruptive acts."[59] A domestic authority with law enforcement power categorizing civil disobedience as unlawful is antithetical to freedom and a precursor for privacy violations. Individuals on the Key Activist list were subject to technical and physical surveillance despite not being suspected of committing or planning to commit a federal crime.[60]

[52] Ibid., at 55.

[53] Ibid., at 55.

[54] Ibid., at 55.

[55] Ibid., at 90.

[56] Ibid., at 90.

[57] Ibid., at 90.

[58] Ibid., at 90.

[59] Ibid., at 90.

[60] Ibid., at 90.

The FBI abolished the Agitator Index in 1971 because the Agency was already conducting surveillance on those people under the decades old Security Index. The FBI and Department of Justice (DOJ) created the Security Index as part of an emergency action plan; if a significantly disruptive event occurred that threatened the effective operation of national, state, or local governments or of national defense, the FBI would immediately detain the individuals on this list without warrant. The Church Committed found that to place someone on the Security Index, the FBI required no more than a "reasonable ground to believe that such person probably will engage in, or probably will conspire with others to engage in, acts of espionage and sabotage, including acts of terrorism or assassination"[61]—or any other act that could create a significant disruptive event. Despite the FBI tightening the Security Index's standards and reducing its size in 1955, those names taken off were simply placed on the Communist Index. In 1960, the FBI renamed the Communist Index the Reserve Index and expanded it to include professors, teachers, labor union organizers, newsmen, lawyers, doctors, and scientists. The Reserve Index served as a list of people who would receive priority consideration for action by the FBI after it detained those listed on the Security Index.[62]

2. Privacy Implications

Every program detailed above expanded beyond its original mission to include, if not exclusively focus on, domestic intelligence. Two major components of the privacy costs weighed against these programs were the number of Americans affected and the low intelligence value. For example, by the time the CIA terminated CHAOS its surveillance had included radical students, African-American expatriates, and U.S. persons that traveled to certain overseas locations.[63] More concretely, through CHAOS operations the CIA had indexed information on over 300,000 people and groups and created 13,000 files that included more than 7,200 files on Americans and over 100 on domestic groups.[64] The Committee concluded that the program's collection was

[61] Ibid., at 92.

[62] Ibid., at 54–56,69,89,91–92.

[63] Ibid., at 100.

[64] Ibid., at 6,102.

excessive and that much of the information was irrelevant to legitimate intelligence and government interests.[65]

In the end, the Committee's report found that the CIA mail-opening program produced a computerized index of nearly 1,500,000 names. The Senate hearings on mail opening revealed that during the span of these operations, 28,322,796 letters were subject to screening, of which the CIA photographed 2,705,726 envelopes, copied 389,324 envelopes, and copied the contents of 215,820 letters it had opened. During the hearings, the Church Committee struggled to find a single case of these operations resulting in the identification of a foreign agent. In addition, internal IC reports scrutinized at the hearings showed that the information was only occasionally helpful, a meager source of intelligence, and of very little value. The Church Committee report concluded that the CIA intercepted communications of various types of domestic dissidents through the mail opening programs that was unrelated to foreign intelligence or counterintelligence purposes.[66]

The NSA's MINARET and SHAMROCK programs received similar criticisms. The Church Committee found it difficult to attribute any meaningful intelligence value to MINARET.[67] For example, the NSA intercepted, disseminated, and stored communications that were mostly of a private or personal nature, such as peace protestors, anti-war activists, journalists, and a spouse of a U.S. senator, or about rallies and demonstrations that were already public knowledge.[68] While the 1,600 names on the MINARET watch list was small compared to the scope of other programs, the collection was still quite substantial.[69] The Committee did not reveal as many specifics about the NSA programs as it did for the others. What is likely is that SHAMROCK essentially operated as a collection method for acquiring SIGINT on Americans on the MINARET watch list. Under the SHAMROCK program, the NSA selected approximately 150,000

[65] Ibid., at 102.

[66] Ibid., 6,59,108; *Hearing on Mail Opening*, 1–2,6,31,168.

[67] S. Rep. No. 94-755, at 108 (1976).

[68] Ibid., at 108–09.

[69] Johnson, *Retrenchment and Reform*, 85.

messages per month for additional analysis.[70] Being that the MINARET list was composed of mostly Americans, the overall effect was the NSA monitoring a pervasive amount of citizens' private communications.

The various FBI programs resulted in widespread surveillance of Americans. Between 1960 and 1974, of the over 500,000 separate investigations of subversive persons or groups, not a single person or group was prosecuted under the relevant laws that prohibit overthrowing the government—the very legal basis used to conduct these investigations.[71] Prosecutions based on other laws were also scarce. For example, only 1.3 percent of the 17,528 domestic intelligence investigations by the FBI in 1974 resulted in prosecution and conviction.[72] Moreover, the 500,000 number represents only the investigations carried out by headquarters and does not include those conducted by the FBI field offices, which maintained a larger number of investigative files.[73] Not only were the total investigations likely much higher, but so was the number of people affected. Domestic intelligence files contained information on more than one person or group.[74] The Church Committee found that hundreds or thousands of group members or associates could be included in a single file.[75]

Another major component of the privacy costs associated with these programs was the breakdown between foreign intelligence agencies and domestic law enforcement. The Committee specifically noted how the CIA programs violated the ban on foreign intelligence agencies from conducting internal security, as well as violating statues that protect mail privacy and prohibit the interception of communications.[76] The NSA bypassed several similar restrictions, such as those establishing that it only collect foreign intelligence and monitor only foreign communications, but not communications between

[70] Ibid., 84.

[71] S. Rep. No. 94-755, at 19 (1976).

[72] Ibid., at 19.

[73] Ibid., at 6,47.

[74] Ibid., at 6.

[75] Ibid., at 47.

[76] Ibid., at 12,58–59.

persons within the United States or concerning purely domestic affairs.[77] Regardless of these rules, the NSA conducted domestic intelligence. Not only were the CIA and NSA programs almost exclusively providing intelligence for domestic law enforcement purposes, but many of the investigations they supported were illegitimate. For example, the FBI, the main provider of names to the watch lists, used the NSA to collect SIGINT on domestic terrorists, foreign radical suspects, journalists, civil rights leaders, and politicians such as high profile targets Art Buchwald, Martin Luther King, Jr., and Frank Church.[78] All of these programs intentionally neglected privacy protections for American citizens. The CIA, NSA, and FBI collectively eroded the institutional design to separate foreign and domestic intelligence as a means of protecting American's against intrusive government power.[79] These effects provided much of the impetus behind Senator Church's push for legislative changes to insure intelligence abuses would not occur again.[80]

The final major privacy concern raised by these intelligence programs was the blatant disregard for constitutional protections. The widespread privacy infringements violated the constitutional rights of Americans engaged in lawful activity.[81] As the record shows, these domestic intelligence activities did not focus on collecting evidence for criminal investigations but instead became a process of conducting illegal surveillance and secret activities against American citizens.[82] People were targeted by the government for First Amendment protected activities such as political expression and lawful assembly.[83] Government surveillance and intimidation both infringed on privacy and deterred citizens from exercising their First Amendment rights.[84]

---

[77] Ibid., at 69,104.

[78] Johnson, *Retrenchment and Reform*, 85.

[79] S. Rep. No. 94-755, at 104 (1976).

[80] Johnson, *Retrenchment and Reform*, 94–95.

[81] S. Rep. No. 94-755, at 1,15 (1976).

[82] Ibid., at 10,63,86.

[83] Ibid., at 1,10,17,20,68.

[84] Ibid., at 1,10,17,20.

The widespread abuses by the intelligence agencies resulted in the overhaul of executive, congressional, and judicial intelligence oversight. In the summer of 1975, President Gerald Ford implemented mechanisms to better supervise CIA activities, restricted CIA's domestic activities, banned mail opening, and ended the abusive wiretaps and use of tax information.[85] President Ford also issued Executive Order 11905 in February 1976, which established an Intelligence Oversight Board within the Executive Office of the President.[86] Congress followed suit. The Senate created the Select Committee on Intelligence in May of 1976 and the House of Representatives established the Permanent Select Committee on Intelligence in July of 1977.[87] Congress empowered both Committees with oversight of the IC and the power to authorize expenditures for intelligence activities.[88] Another key change was the 1978 Foreign Intelligence Surveillance Act (FISA) that put strict legal conditions on the IC's use of electronic surveillance and established the FISA Court (FISC) as the approving authority for such surveillance.[89] Finally, the Intelligence Oversight Act of 1980 established the criteria for intelligence reporting to the oversight committees, which included disclosing covert actions and the loose standard of keeping the committees fully and currently informed.[90] All of these reforms produced the cumulative effect of placing the IC "within the constitutional scheme for controlling government power"[91] and created an overlay of oversight bodies focused on better protecting civil liberties.[92]

B. TOTAL INFORMATION AWARENESS

In 2002, the Defense Advanced Research Agency (DARPA), an organization within the Department of Defense (DOD), announced it was developing new intelligence

[85] "The Evolution of the U.S. Intelligence Community-An Historical Overview," Federation of American Scientists, accessed March 2, 2014 http://www.fas.org/irp/offdocs/int022.html.

[86] Ibid.

[87] Ibid.; Johnson, *Retrenchment and Reform*, 108.

[88] "Evolution of the U.S. Intelligence Community," Federation of American Scientists.

[89] Ibid.

[90] Ibid.

[91] S. Rep. No. 94-755, at iii (1976).

[92] Johnson, *Retrenchment and Reform*, 108–09.

technologies under its TIA initiative.[93] In September 2003, the program ended after suffering public, media, and Congressional backlash.[94] At the core of the TIA controversy was its improper balance between security and privacy. The TIA experience thus provides an example of a national security program that ended due to unacceptable privacy costs.

1. Capabilities

Immediately following 9/11, national leaders focused on the need to break down the barriers between IC partners, increase intelligence sharing, and improve the ability of the IC to connect disparate fragments of intelligence. The TIA program, as envisioned, was the theoretical answer to these problems. The goal of TIA was to create a counterterrorism information architecture that would: increase access to and sharing of information, thereby increasing how much total information was available and could be evaluated; provide automatic warnings of dangerous or suspicious activity after a trigger event occurred; cue analysts about peoples' activities that match terrorist behavioral patterns; enable hypothesis testing of theories and mitigation strategies related to future terrorist activities.[95] Increasing access, sharing, and coverage of information were technical solutions to having data and analysts dispersed throughout the world. Trigger events and behavioral patterns were also technical solutions in which computers would have analyzed vast amounts of transactional and behavioral data and then provide warnings of suspicious activity.

Procedurally, TIA would have started with a red team developing different terrorist attack scenarios against the United States, determine what planning and preparation activities these attacks require, create a list of expected transactions that

---

[93] John Markoff, "Pentagon Plans a Computer System that Would Peek at Personal Data of Americans," *New York Times*, November 9, 2002, http://www.nytimes.com/2002/11/09/politics/09COMP.html.

[94] H.R. Rep. No. 108-283, at H8772 (September 24, 2003) (Conf. Rep.).

[95] Defense Advanced Research Projects Agency (DARPA), *Report to Congress regarding the Terrorism Information Awareness Program*, May 20, 2003, 3–4. Note that the name changed from Total Information Awareness to Terrorism Information Awareness. These two names are interchangeable and refer to the same program, according to H.R. Rep. No. 108-283, at H8772 (September 24, 2003) (Conf. Rep.).

would fit these models, and analyze what behavioral patterns a terrorist would likely follow for a given attack scenario.[96] For such a program to work, however, would have required intelligence analysts to have access to a considerable amount of data not only on known or suspected terrorists, but also on everyone else. In order to differentiate between the average person, the person who is neither average nor a terrorist, and the terrorist required monitoring the activities of everyone. Distinguishing the terrorists and their activities from the general population required a set of tools, which were the new technologies DARPA planned to develop as subprograms of TIA.[97] The technologies with the most notable privacy concerns were Genisys, Evidence Extraction and Link Discovery, Scalable Social Network Analysis, MisInformation Detection, Human Identification at a Distance, Activity, Recognition and Monitoring, and Next-Generation Face Recognition.[98]

a. Genisys

The purpose of the Genisys program was to develop the technology necessary to integrate databases and other information sources. At the time, the available technology was too complex, inflexible, slow, and error prone; making integrating or creating databases on a scale required by the IC extremely difficult to achieve. By developing a federated database architecture, Genisys would have enabled analysts to access, use, and evaluate more information. The program would have integrated data related to "all potential terrorists and possible supporters; terrorist materials; training, preparation, and rehearsal activities; potential targets; specific plans; and the status of [U.S.] defenses."[99] Genisys was a program designed to connect the dots for an IC that was heavily criticized for failing to do so before 9/11; it would have done this by developing groundbreaking ways of accessing and sharing unprecedented amounts of information at as close to real time as possible.[100]

---

[96] DARPA, *Report to Congress*, 3, 6, 18–31.

[97] Ibid., 3.

[98] Ibid., 31.

[99] Ibid., A-10.

[100] Ibid., 5–6,A-10.

b. Evidence Extraction and Link Discovery

The technologies DARPA slated for development under the Evidence Extraction and Link Discovery (EELD) program would have taken unstructured textual data from sources ranging from intelligence to news reports and automatically extract information about relationships between people, organizations, and places. Its anticipated intelligence value would have been to minimize the analysis of legitimate activities and focus instead on those the system automatically flagged as suspicious. The automated analysis of various sources could have potentially discovered new threats from unknown individuals or groups. Conceptually, it would have automatically found the dots, decided which dots to connect, and connected them.[101]

c. Scalable Social Network Analysis

The objective of Scalable Social Network Analysis (SSNA) was to improve social network analysis capabilities by identifying normal patterns of behavior, patterns that match the behavior of terrorist groups, and changes in a terrorist network that indicate an impending attack.[102] The intelligence value of this program was basic, but important: in order to defeat a terrorist network, intelligence must first detect and define that network. It would have required essentially the same type of information as the EELD program—namely, information that defined or explained the relationships between people, organizations, and places. The SSNA program would have included information that characterizes the type of interactions between people, the nature of the interaction, and the different roles people have in a social network.[103]

d. MisInformation Detection

The focus of the MisInformation Detection (MInDet) program was to determine the intelligence reliability of publicly available sources and identify intentional misinformation efforts against the IC.[104] While this would have had a general

[101] Ibid., 7–8.

[102] Ibid., 9.

[103] Ibid., A-16.

[104] Ibid., 9.

intelligence value in the form of vetting open sources, another application of the program could have provided a much more specific counterterrorism value. Based on the premise that terrorists and their supporters would intentionally try to hide information about themselves and their activities, the proposal for MInDet envisioned the potential for the program to detect deceptive information on government forms and in textual documents, which could then prompt a more thorough investigation into the person's activities.[105]

e. Human Identification at a Distance

The purpose of Human Identification at a Distance (HumanID) was to advance biometric technologies "with the capability to detect, recognize, and identify humans at a distance."[106] In essence, the program would have monitored people near government facilities with video, infrared imagery, and multispectral sensors, collect their biometric signatures, uniquely identify them, and presumably provide a reliable assessment on whether or not a person was threatening. DARPA described the intelligence value of this program as providing critical early warning against human-based threats, such as terrorism.[107]

f. Activity, Recognition and Monitoring

Where HumanID focused on the individual biometrics, Activity, Recognition and Monitoring (ARM) sought to develop technologies to capture, identify, and classify different types of human activities in a surveillance environment.[108] The intelligence value of this program would have been to differentiate normal and suspicious human behaviors in a given area or situation and then provide a warning when it detected questionable behavior. For example, it potentially could have identified unattended packages at a public event or terrorists casing a critical infrastructure target.[109] The ARM program would have relied on similar sources as HumanID, to include video, agile

[105] Ibid., 9.

[106] Ibid., 10.

[107] Ibid., 10–11.

[108] Ibid., 11.

[109] Ibid., A-21.

sensors, low power radar, infrared sensors, and radio frequency tags.[110] An implied capability was the ability to monitor the routine behavior of average citizens in order to develop the baseline human activity models on which this relies. Additionally, the ARM program also implied constant surveillance in public places, as the collection technologies would feed the automated warning components of the system.

g. Next-Generation Face Recognition

The Next-Generation Face Recognition (NGFR) program pursued development of new facial biometrics collection and analysis tools. After developing the technology, NGFR would have been able to automatically and confidently identify known or suspected individuals detected by a web of sensors. Implied in this program would have been its integration with the HumanID and ARM surveillance sensors against which to run the facial recognition technology. An additional major component of the NGFR program would have been to create a large database of facial imagery.[111]

h. Composite Capabilities of the Total Information Awareness Program

Taking all of the subprograms into account, two characteristics of TIA stand out. First, there was a robust virtual surveillance component. Genisys would have established the information network that provided access to incomparable amounts of data on terrorists, criminals, and law abiding American citizens. The EELD program would have then used Genisys' database infrastructure to sift through the treasure trove of information and automatically decipher links between people, places, and organizations. In essence, it would automatically build the social network of whomever the analyst queries. Applying the SSNA program would better refine that person's network and use automated tools to determine if that person's social network is legitimate or resembles a terrorist group. Finally, although the MInDet program is not directly connected to the chain of virtual surveillance, automatically scrutinizing government documents and publicly available information could provide the impetus for starting an investigation into

[110] Ibid., 11.

[111] Ibid., 12.

someone's behavior by indicating to the EELD or SSNA programs that this person's activity is questionable.

Second, TIA included robust physical surveillance capabilities. Common to both HumanID and NGFR would have been the ability of the government to use a distributed web of complex sensors across numerous facilities and public environments to uniquely identify people. In order for these programs to work, each would have to communicate with a database of personally identifiable biometric data in order to establish an identity. In addition, the ARM program would have provided the capability to flag suspicious activity detected on the same network by comparing a person's behavior with models of what it considered suspicious. Yet to do this required substantial surveillance of routine, law-abiding behavior in order to establish a baseline of non-threatening behavior. Such were the proposed virtual and physical capabilities of TIA; the privacy implications were many.

2. Privacy Implications

Criticisms of TIA included accusing DARPA of creating a dragnet, Big Brother spying program against Americans that was outside of congressional oversight and lacked sufficient safeguards, constitutional protections, clear accountability, and privacy related guidelines.[112] These claims had merit, but so did DARPA's defense of TIA. The program was in the developmental stage and under an agency whose focus was to create the new technologies required to fill intelligence capability gaps. Since TIA was a conceptual research and development program, DARPA argued there were practical reasons why robust privacy mechanisms were not yet built into the system. This is not to say that DARPA ignored the privacy concerns raised by TIA. On the contrary, DARPA repeatedly addressed the privacy implications in its description of TIA subprograms and was developing the Genisys Privacy Protection program as part of TIA.[113] Nevertheless,

[112] Ron Wyden, "Wyden Calls for Congressional Oversight, Accountability of Total Information Awareness Office," news release, January 15, 2003, http://www.wyden.senate.gov/news/press-releases; Timothy J. Burger, "A Terror Tracking System by Any Other Name," *TIME*, May 14, 2003, http://content.time.com/time/nation/article/0,8599,451925,00.html; Markoff, "Pentagon Plans a Computer System that Would Peek at Personal Data of Americans."

[113] DARPA, *Report to Congress*, 3,6,18–31.

the reservations associated with TIA were so substantial that Congress defunded the program.

From DARPA's perspective, the principal concerns raised by TIA came from the programs with data access, data search, and pattern recognition capabilities—namely, Genisys, EELD, SSNA, MInDet, HumanID, ARM, and NGFR. The core privacy issues with HumanID, ARM, and NGFR related to program effectiveness and accuracy, where and when the technologies would be deployed, and if the programs would analyze stored surveillance of public places. These concerns, however, were secondary to those created by the Genisys, EELD, SSNA, and MInDet data search and analysis tools, which focused on the type of information stored in the programs' databases.[114]

In addition to program specific implications, DARPA also identified broad level privacy concerns. Chief among these were access to sensitive personal information, access to aggregate personal information, storing personal information, unauthorized access to or use of the sensitive information, and accuracy of the personal information.[115] The level of attention given to privacy concerns and DARPA's plan for addressing them reflects that the agency was serious about creating protections in tandem with the other technologies. Its development of tools to limit searches to legally authorized results, provide an automated audit trail of searches and record retrieval, and make the data anonymous demonstrated this commitment.[116] These tools were part of a program called Genisys Privacy Protection, which would have also been part of TIA.[117]

A Department of Defense IG report conducted in response to a request from Senators Chuck Grassley, Bill Nelson, and Chuck Hagel offers another perspective on the privacy implications of TIA. The IG report identified two significant privacy concerns with TIA not addressed in DARPA's analysis. First, DARPA did not conduct a privacy impact assessment (PIA). DARPA defended the choice not to conduct a PIA based on its use of artificial data and legally obtained intelligence; this type of information did not

[114] Ibid., 3,31.

[115] Ibid., 29–30.

[116] Ibid., 33–34.

[117] Ibid., 6–7,A-12–13.

require an assessment.[118] While the IG conceded that DARPA's argument was technically correct, it nonetheless concluded that "in the case of TIA, prudence would dictate that a requirement for a privacy impact assessment be done as a best business practice."[119] The IG's argument focused on three core points: when aggregated, the information would have been used for purposes other than the original intent; development of TIA technologies occurred simultaneously with its transition to operational status; TIA would have been used for domestic law enforcement purposes.[120] The use of artificial data was irrelevant because the intelligence technologies were shifting into operational status, after which hypothetical privacy issues shifted to actual privacy violations. The other significant privacy issue addressed by the IG was the use of Department of Defense assets for domestic purposes: "the use of TIA by law enforcement is what has caused the greatest public concern over privacy."[121] The fear was that TIA created a substantial increase in government power precisely in the section of government with law enforcement authority; the program was primed for abuse and misuse.[122]

One noteworthy privacy concern brought up in public criticism of TIA was the nature of the information. Allegations of Big Brother, dragnet surveillance came out of TIA's scope of collection as well as the type of information it would use. Identifying patterns of behavior, monitoring for automatic triggers of suspicious behavior, and similar activities mentioned in the capabilities section above require substantial collection of and access to transactional data. The types of data that DARPA would have used under TIA were financial records, educational documents and information, travel activities, medical records, transportation history, housing information, email and telephone

[118] U.S. Department of Defense, Office of the Inspector General, *Terrorism Information Awareness Program*, D-2004-033, December 12, 2003, 4–6.

[119] Ibid., ii,4–6,14.

[120] Ibid., 6,11.

[121] Ibid., 7.

[122] Ibid., 4.

records, credit card purchases, and countless government records.[123] Access to these transactional records would have resulted in making available to intelligence and law enforcement agencies commercial and government records on a colossal scale. Permitting the executive branch to collect and access this personal information creates a considerable privacy infringement. Although DARPA argued that TIA would not include dossiers on U.S. citizens nor maintain a single grand database of all U.S. transactions,[124] such a technical distinction was immaterial. DARPA recognized that TIA would have eliminated the virtual obscurity of having personal data spread throughout different sources and formats through providing almost instantaneous access to all these data.[125] Rapid access to various sources of sensitive personal information would have achieved the same functional purpose of dossiers but in the form of search results, and of a grand database but in the form of broad access to multiple databases. It is therefore necessary to factor in privacy concerns derived from what information reveals about a person when aggregated with numerous sources.

C. CONCLUSION

The Cold War era CIA, NSA, and FBI intelligence activities as well as the post-9/11 TIA subprograms represented unacceptable infringements on privacy. Society, as the stakeholder in privacy interests, rejected certain government behavior as having too high of a cost. It is not to say that every national security program must have the expressed approval of the people, but it is to say that some things are unacceptable. Measuring privacy costs therefore requires applying these lessons by avoiding the unacceptable costs and working toward the threshold of what is acceptable. More of this

---

[123] "Total Information Awareness (TIA) System," DARPA, last updated November 25, 2002, http://www.darpa.mil/iao/TIASystems.htm (site discontinued, a screenshot is available at http://epic.org/events/tia_briefing/tia_screenshot.gif); "TIA Categories," DARPA, last updated November 25, 2002, http://www.darpa.mil/iao/TIASystems.htm (site discontinued, a screenshot is available at http://epic.org/events/tia_briefing/tia_categories.gif); Gene Healy, "Beware of Total Information Awareness," *CATO*, January 20, 2003, http://www.cato.org/publications/commentary/beware-total-information-awareness; Jeffrey Rosen, "Total Information Awareness," *New York Times*, December 15, 2002, http://www.nytimes.com/2002/12/15/magazine/15TOTA.html; Markoff, "Pentagon Plans a Computer System that Would Peek at Personal Data of Americans."

[124] DARPA, *Report to Congress*, A-6.

[125] Ibid., 33.

will be addressed in Chapter IV. What suffices at this point is to recognize that there are historically founded characteristics of inappropriate government behavior. Before discerning the boundaries on privacy costs, it is first necessary to address the second primary factor of measuring privacy costs: the expectation of privacy. Whereas society's standards temper government action, the government's interest in protecting society shapes what is a reasonable expectation of privacy. It is to this issue that this thesis now turns.

THIS PAGE INTENTIONALLY LEFT BLANK

III. EXPECTATION OF PRIVACY

The thesis now turns to the second of the two primary issues that affect privacy costs: an expectation of privacy. One way to assess privacy costs is to ascertain if a person has a valid privacy interest and determine if a surveillance program infringes on that interest. This interest is commonly referred to as an expectation of privacy, which is based on a person exhibiting a subjective expectation of privacy and society's willingness to accept that expectation as reasonable.[126] Interpretations of what satisfies these two standards are rooted in Supreme Court cases from the 1970s and have become outdated. The changing information landscape requires a shift in the subjective and reasonable standards of privacy in order to fully account for the privacy costs of modern surveillance programs. This chapter will demonstrate that there is an increase in personal information available to surveillance programs, which brings with it significant privacy implications. It will conduct a brief analysis of the subjective and reasonable standards of the expectations of privacy followed by an argument for how the pervasiveness of technology in modern society challenges traditional interpretations of these two conditions. The chapter will conclude by offering new standards for evaluating a subjective and reasonable expectation of privacy that will result in a more accurate assessment of privacy costs.

A. SUBJECTIVE AND REASONABLE PRIVACY STANDARDS

The Supreme Court developed the expectation of privacy standards as a way to gauge if a person has a Fourth Amendment privacy interest that protects him or her against unwarranted domestic surveillance. Starting in Katz versus United States, the Court applied a twofold test to ascertain if a person has a valid privacy interest: "first that a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[127] A subjective expectation hinges on what actions a person takes to exhibit his or her intent to

[126] *Katz v. United States*, 389 U.S. 347 (1967).

[127] Ibid.

maintain privacy, such as the things a person keeps to him or herself. In his concurring opinion in Katz, Justice John Marshall Harlan II argued that a person must demonstrate an intention to keep objects, activities, or statements to himself in order to claim an expectation of privacy.[128] Similarly, Justice Byron White argued that the intent to preserve privacy is reflected by a person's efforts to exclude the uninvited ear.[129] While these actions certainly demonstrate a person's intent to keep something private, the effect is to substitute secrecy for privacy. Both justices Harlan and White maintained that sharing information negates a subjective expectation of privacy.[130] This interpretation of what constitutes a subjective expectation of privacy contradicts the fundamental purpose of the Fourth Amendment. Constitutional privacy safeguards are designed to protect a person against government inference in his or her life,[131] which entails substantially different considerations than the burdensome requirement that everyone must keep everything secret. Put a different way, it is not that a person has a right to keep things secret; it is that he or she is free from unwarranted government intrusion. The problem with demanding secrecy in order to maintain a privacy interest is it erodes privacy protections by setting an infeasible requirement, thereby giving the government access to information that it can argue does not raise privacy costs because there is no legitimate privacy interest.

A valid privacy interest requires not just a person exhibiting a subjective expectation of privacy, but society must recognize it as reasonable. The most influential interpretation of what society will accept as a reasonable expectation of privacy is known as the third party doctrine. The doctrine was established in the cases Smith versus Maryland and United States versus Miller, in which the Supreme Court held that society rejects an expectation of privacy when a person voluntarily provides information to a third party. The two premises of the Court's conclusion were that voluntarily providing information to a third party does not exhibit a subjective expectation of privacy and the

[128] Ibid.

[129] Ibid.

[130] Ibid.

[131] Ibid.

person providing the information accepts the risk that it will be given to the government.[132] One problem with this opinion is it builds upon the flawed understanding of privacy as secrecy by granting the government unfettered access to any information a person divulges. Another problem is it undermines basic freedoms because it establishes that a person must isolate herself from modern society in order to maintain her privacy interest. In a free society, however, providing information to another party during routine societal interactions is not the same as a person consenting to government access to that information.[133] In the words of Justice Marshall's dissenting opinion in Smith: "privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[134] It is unreasonable for society to align its standards of privacy with a paranoid expectation that the other party will provide any and all information to the government. The traditional application of the reasonable standard results in the categorical rejection of valid privacy interests for information provided to third parties, which unduly decreases privacy costs associated with government surveillance.

While this thesis agrees in principle with the subjective and reasonable requirements of privacy, it disagrees with the traditional interpretations and applications explained above. The strict, burdensome criteria extend the threshold for establishing a valid a privacy interest beyond what is feasible in modern society. The pervasiveness of technology in America today presents new challenges to what is a subjective and reasonable expectation of privacy. In United States versus Jones, Justice Samuel Alito noted that as technology progresses, there will not always be clear analogies between the twenty-first and eighteenth centuries.[135] The role of various technologies in routine societal interactions is such a situation, and it requires a new way of interpreting what constitute subjective and reasonable expectations of privacy.

---

[132] *United States v. Miller*, 425 U.S. 435 (1976).

[133] *Smith v. Maryland*, 442 U.S. 735 (1979).

[134] *Smith*, 442 U.S. 735.

[135] *United States v. Jones*, 132 S. Ct. 945 (2012).

B. THE PRIVACY IMPLICATIONS OF TECHNOLOGY IN SOCIETY

a. More Internet Usage

The reach of technology into nearly every part of the American way of life and the amount of records kept by both people and organizations has important privacy implications. Some of the most basic social interactions, such as working, banking, shopping, commuting, and communicating, now have a cyber element. Recent statistics put the amount of Americans with Internet access at 86 percent of the population.[136] The level of use alone reflects the pervasiveness of the Internet in society. When the types of online activities are taken into account, the role of technology in the performance of routine social interactions becomes apparent (Table 1).

136 "Internet User Demographics," Pew Research Center, accessed February 8, 2014, http://www.pewinternet.org/data-trend/internet-use/latest-stats/; Center for the Digital Future, *The 2013 Digital Future Report: Surveying the Digital Future*, Los Angeles, CA: University of Southern California, 2013,15, http://www.worldinternetproject.net/_files/_Published/_oldis/713_2013_digital_future_report_usa.pdf.

Have Used the Internet To:	Percentage of Internet Users
Find information through a search engine	91
Send or receive email	88
Search a map or get driving directions	84
Read the news	78
Research health information	72
Look for information on a local, state, or federal government website	67
Social networking	67
Make travel reservations or purchases	65
Purchase books	63
Read political news or information	61
Conduct online banking	61
Look for religious information	32

Table 1. U.S. Internet Usage[137]

b. More Participants and Data

Most of the traditional ways of carrying out social interactions included just two parties. For example, purchasing a book used to be between a person and a bookstore, buying an airline ticket between a person and an airline, and banking between a person and the bank. Conducting these activities over the Internet, however, increases the number of participants for any given exchange. A routine interaction would now reasonably include the person, the Internet service provider, a search engine, the company that builds or maintains the website, and the company or organization with whom the person intends to interact. These participants may keep records on the person and his or her activity. Thus, with the increase in participants in ordinary transactions has also come an increase in data creation. An estimated 98 percent of stored information was digital as of 2013 and technological improvements have simultaneously amplified

137 "Trend Data (Adults)," Pew Research Center, accessed February 8, 2014, http://www.pewinternet.org/Trend-Data-(Adults)/Online-Activites-Total.aspx; "Pew Internet: Health," Susannah Fox, Pew Research Center, December 16, 2013, http://www.pewinternet.org/Commentary/2011/November/Pew-Internet-Health.aspx; Center for the Digital Future, *The 2013 Digital Future Report*, 16.

information access, storage, sharing, and analysis capabilities.[138] Traditional interpretations of the subjective and reasonable expectations of privacy deny that a person has a valid privacy interest in any of these interactions or any of the information.

There are also the hidden, less known participants that constantly track online activity. Data brokers surreptitiously collect and aggregate data pertaining to a person's online activity, which they then use to create detailed dossiers about him or her.[139] Companies like Acxiom, Epsilon, Reed Elsevier, and Datalogix each maintain data on millions of Americans.[140] One of the primary methods these companies use to track a person's behavior is through websites, but tracking can also occur through mobile devices.[141] This tracking occurs mostly unknown because it requires no deliberate consent by the user, the technology is embedded in the websites, and it uses the unique identifiers associated with a person's device.[142] When someone uses the Internet to read the news, make travel reservations, and do online banking, his or her activity is tracked across multiple websites. For example, the Doubleclick tracking tool monitors users' behavior on websites belonging to Bank of America, Delta airlines, Enterprise and Hertz rental car, Hilton hotel, CNN, Fox News, and the Washington Post.[143] Similarly, Omniture tracks activity on Bank of America, Citi Bank, JP Morgan, Budget rental car,

---

[138] U.S. Senate, Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, December 18, 2013, 1.

[139] Ibid., i,5,36.

[140] Ibid., 10,12.

[141] Ibid., 10,31.

[142] Ibid., 4,31.

[143] Bank of America homepage, accessed February 7, 2014, https://www.bankofamerica.com/; Delta homepage, accessed February 7, 2014, http://www.delta.com/; Enterprise homepage, accessed February 7, 2014, http://www.enterprise.com/car_rental/home.do; Hertz homepage, accessed February 7, 2014, https://www.hertz.com/rentacar/reservation/; Hilton homepage, accessed February 7, 2014, http://www3.hilton.com/en/index.html; CNN homepage, accessed February 7, 2014, http://www.cnn.com/; Fox News homepage, accessed February 7, 2014, http://www.foxnews.com/; Washington Post homepage, accessed February 7, 2014, http://www.washingtonpost.com/.

Marriott hotel, BBC News, Fox News, and the Washington Post.[144] The companies that own these trackers partner together and share the information collected.[145] Thus, even if a specific tool such as Omniture does not track a user's activity across all websites, partnership significantly increase its access to information. The associated business records about a person's activities would be outside of the traditional application of the reasonable privacy expectation of privacy standard, even though a person did not voluntarily provide this information.

c. More Personal

The information in business records that pertain to online activity can be highly personal. Today, these records reveal a significant amount of private details, such as a person's habits, preferences, and financial and health status.[146] By tracking routine activities, companies are able to paint an accurate profile of the user. Bluekai, for example, claims: "place our pixel on any page to analyze incoming traffic [and] discover the precise aggregate profile of any site visitor."[147] Although this statement seems more ambition than reality, the amount of data that each of the hundreds of companies track and the level of sharing that occurs through partnerships makes the precise profiling of users feasible. Acxiom's consumer profiles demonstrate this point. Acxiom requires a user to enter his first and last name, full address, date of birth, last four digits of his social security number, and an email address in order to see some of the information it has on

---

144 Bank of America homepage, accessed February 7, 2014, https://www.bankofamerica.com/; Citi Bank homepage, accessed February 7, 2014, https://online.citibank.com/US/Welcome.c; J.P. Morgan homepage, accessed February 7, 2014, https://www.jpmorgan.com/pages/jpmorgan; Budget homepage, accessed February 7, 2014, http://www.budget.com/budgetWeb/home/home.ex; Marriott homepage, accessed February 7, 2014, http://www.marriott.com/default.mi; *BBC News*, accessed February 7, 2014, http://www.bbc.com/news/; Fox News homepage, accessed February 7, 2014, http://www.foxnews.com/; *Washington Post* homepage, accessed February 7, 2014, http://www.washingtonpost.com/.

145 "Partners," Foresee, accessed on March 1, 2014, http://www.foresee.com/company/partners.shtml; "Webtrends Partners," Webtrends, accessed on March 1, 2014, https://webtrends.com/partners/webtrends-partners; "Partner Program," Bluekai, accessed on March 1, 2014, http://bluekai.com/customers.php; "Technology Partners," Brightcove, accessed on March 1, 2014, http://www.brightcove.com/en/partners/technology-partners.

146 Senate Committee on Commerce, *A Review of the Data Broker Industry*, i,2.

147 Bluekai, "Little Blue Book: A Buyer's Guide," Bluekai, February 2014, 5, http://bluekai.com/bluebook/bluekai-little-blue-book.pdf.

him.[148] The requirement to use personally identifiable information in order to see part of a digital dossier makes it evident that the tracking is precise; it is personal.

Two examples demonstrate what even limited data points reveal about a person. One of those sources of information is social network sites. WolframAlpha provides a detailed analysis about a person's life simply by accessing the metadata associated with his or her Facebook account. Its Personal Analytics product will calculate a user's activity patterns, to include when a person is active for a given day of the week, what he or she is doing, such as posting photos or making comments, and if the connection occurs through a mobile device.[149] It will also diagram the social structure of a person's friends (Figure 1), identify who among them plays a special role, and provide a geographic layout of where those friends are in the world (Figure 2).[150]

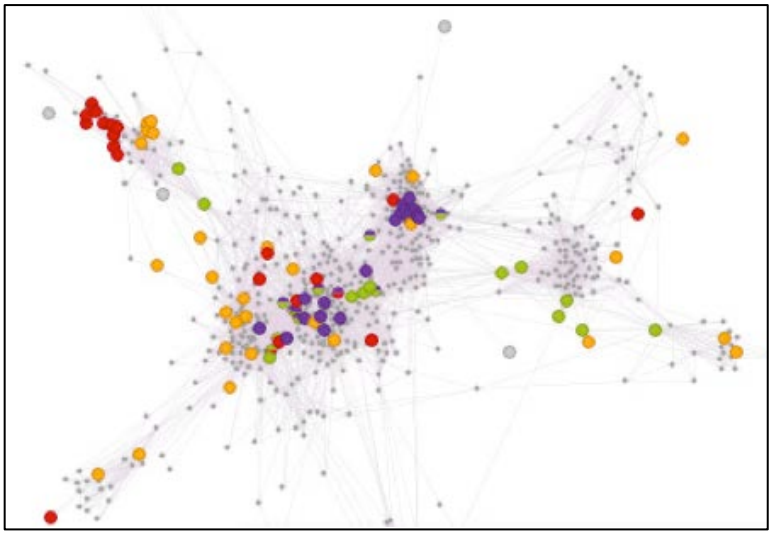

Figure 1. WolframAlpha Social Network Structure Analysis[151]

148 "Who Are you?," Acxiom, accessed on March 1, 2014, https://aboutthedata.com/portal.

149 "Personal Analytics for Facebook," WolframAlpha, accessed on March 1, 2014, http://www.wolframalpha.com/facebook/.

150 Ibid.

151 Figure taken from "Personal Analytics for Facebook," WolframAlpha, http://www.wolframalpha.com/facebook/.

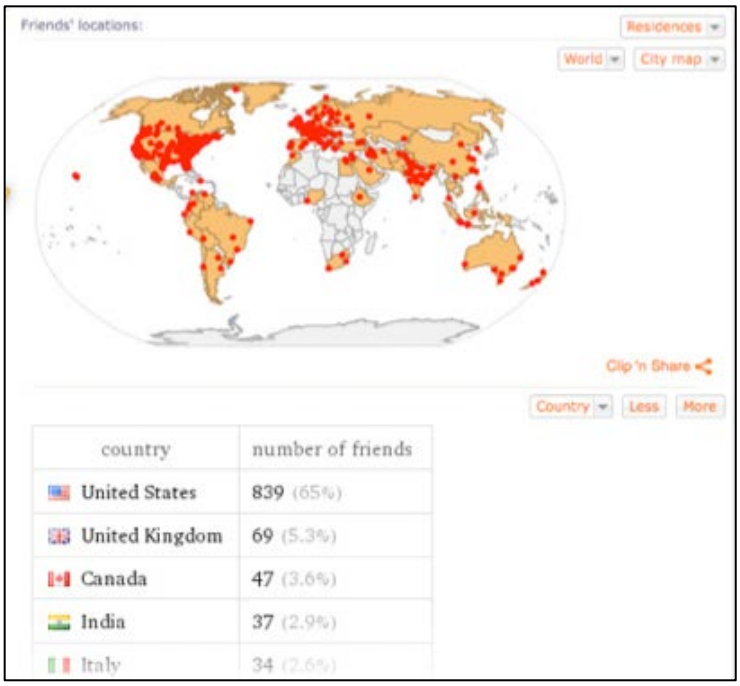

Figure 2. WolframAlpha Friend Location Analysis[152]

Another source that has few details but still reveals significant personal information is email metadata. The Massachusetts Institute of Technology (MIT) Immersion tool analyzes a person's social network based solely on the metadata in his or her emails—the From, To, CC, and timestamp.[153] Based on the analysis of these simple data points, Immersion will show who a person communicates with most, the social network links between the contacts, how far back the communication history goes (Figure 3).[154]

152 Figure taken from "Personal Analytics for Facebook," WolframAlpha, http://www.wolframalpha.com/facebook/.

153 "Immersion: A People-Centric View of Your Email Life," Massachusetts Institute of Technology (MIT), accessed on March 1, 2014, https://immersion.media.mit.edu.

154 "Will Hunting" [Demo], MIT, accessed on March 1, 2014, https://immersion.media.mit.edu/demo.

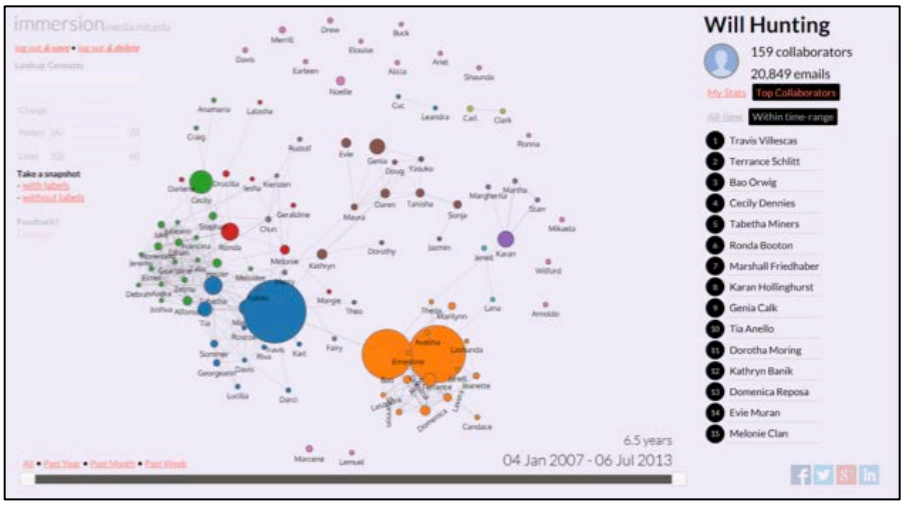

Figure 3. MIT Immersion Email Analysis[155]

Combining the social network and email analysis tools would reveal even more personal information, let alone adding sources of travel, banking, and phone records or sources that track online activity. Providing the government unrestrained access to personal information is extremely worrisome from a privacy perspective, yet that is exactly what results from traditional interpretations of the subjective and reasonable expectations of privacy. Thus, even if the government does not collect this data on Americans or create dossiers, it can access commercial equivalents without a warrant.

C. CONCLUSION

One way to identify privacy costs is to assess the presence of a legitimate privacy interest. Establishing that such an interest exists relies on the two Fourth Amendment privacy standards: a subjective expectation by the individual and society's willingness to recognize that expectation as reasonable. This chapter argued that the traditional interpretations of these two standards have been insufficient, particularly in the context of routine interaction in modern society. The role of technology in society presents a significant challenge because traditional interpretations would authorize government access to a wealth of personal information derived from routine social interactions and that reveals extremely private details. The Fourth Amendment protects a person's privacy

[155] Figure taken from "Will Hunting" [Demo], MIT, https://immersion.media.mit.edu/demo.

from government incursion, but allowing the government free access to this information is in and of itself an incursion. The Court has challenged the traditional interpretations precisely for this reason. While addressing the privacy implications of the third party doctrine in modern society, Justice Sonia Sotomayor argued:

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the email addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every website they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[156]

The purpose of the Fourth Amendment is to ensure the same level of privacy protections for Americans throughout time.[157] In order to do this, there needs to be updated standards of the subjective and reasonable expectations of privacy.

A proper understanding of these two criteria is crucially important because it can skew the balance between privacy and security: if privacy standards are too strict, it will undervalue privacy costs while if the standards are too loose, then it will overvalue privacy costs. This thesis interprets the subjective and reasonable standards to mean the following. First, a person exhibits a subjective expectation of privacy by deliberately limiting the value and quantity of the objects, activities, or statements he or she shares with others and by restricting the number of people with whom he or she shares these things. Second, a reasonable expectation of privacy accounts for the pervasiveness of technology in society, particularly in regards to conducting routine social behaviors, surreptitious collection of personal information, and the level of detail in business records. These standards better capture a person's expectation of privacy, which makes

156 *Jones*, 132 S. Ct. 945 (2012).

157 Ibid.

the overall privacy interest more reflective of actual concerns over privacy infringements. With these two fundamental components of the expectation of privacy established, the thesis will now address how to evaluate the collective privacy costs of a surveillance program.

IV. HOW TO MEASURE PRIVACY COSTS

The analysis in the previous chapters established the elements of privacy costs. Chapter II demonstrated how aspects of intelligence programs that defy Americans' expectations for government behavior can create privacy concerns. Chapter III delineated standards for a subjective and reasonable expectation of privacy against which government activities cannot infringe without generating privacy concerns. Taken as a whole, the factors identified in both chapters provide the basis for measuring privacy costs. This chapter will turn those elements into a model for measuring the overall privacy costs of an intelligence program. The two principal components of this model are the primary and comprehensive assessments.

A. PRIMARY ASSESSMENT

Measuring privacy costs of an intelligence program starts with an analysis of the core privacy elements identified in the previous chapters. This examination first determines whether these elements apply to an intelligence program. Next, it evaluates what effect the presence or absence of that element has on privacy costs. For example, if an intelligence program collects personal information, then there is a legitimate privacy concern, which increases the privacy costs. Some factors decrease the overall cost by accounting for privacy concerns or protecting against abuse. If an intelligence program applies technology that makes information anonymous, for example, then it minimizes the possibility of the government abusing that personal information. On the other hand, the absence of mitigating tools or procedures increases privacy costs. For instance, if limiting the number of analysts who can access sources of personal information lessens the potential for abuse by intelligence agencies, then the absence of this feature increases the possibility for abuse and thus raises the associated privacy cost.

The Privacy Concerns and Safeguards Matrix in Figure 4 is the tool for conducting the primary assessment. As shown in the matrix, privacy cost elements fall into two categories: those that establish privacy concerns and those that act as privacy safeguards. Each factor increases or decreases privacy costs according to the following

general rules. The presence of privacy concerns or the absence of safeguards increases privacy costs. If a program has safeguards, then privacy costs decrease. The absence of a privacy concern neither increases nor decreases costs. For example, a primary assessment of the Cold War FBI programs reviewed in Chapter II would result in the matrix in Figure 5. The comprehensive analysis provides meaning to these costs

Primary Assessment			
Privacy Concerns	**Yes or No**	**Privacy Safeguards**	**Yes or No**
Program collects or accesses personal information:	Yes: Supports valid privacy interest and increased privacy cost	Parties responsible conducted a privacy impact assessment:	Yes = Mitigates privacy concerns and decreases privacy cost
Information collected or accessed is being used for other than intended purpose:	No: Does not support the presence of a valid privacy interest	Sharing of intelligence products derived from personal information is limited:	No = Increases privacy concerns and increases privacy cost
Information falls under a subjective expectation of privacy:		Access to personal information is restricted:	
Society recognizes the expectation of privacy as reasonable:		Program is subject to Executive oversight:	
Information collected or accessed is derived from activities protected under the First Amendment:		Program is subject to Congressional oversight:	
		Program is subject to Judicial oversight:	
		Accountability mechanisms enable the auditing of access to and use of personal information:	
		The information is made anonymous:	

Figure 4. Privacy Concerns and Safeguards Matrix

FBI Cold War Programs

Privacy Concerns	Yes or No	Privacy Safeguards	Yes or No
Program collects or accesses personal information:	Yes	Parties responsible conducted a privacy impact assessment:	No
Information collected or accessed is being used for other than intended purpose:	Yes	Sharing of intelligence products derived from personal information is limited:	No
Information falls under a subjective expectation of privacy:	Yes	Access to personal information is restricted:	No
Society recognizes the expectation of privacy as reasonable:	Yes	Program is subject to Executive oversight:	Yes
Information collected or accessed is derived from activities protected under the First Amendment:	Yes	Program is subject to Congressional oversight:	No
		Program is subject to Judicial oversight:	No
		Accountability mechanisms enable the auditing of access to and use of personal information:	No
		The information is made anonymous:	No

Figure 5. FBI Cold War Programs[158]

B. COMPREHENSIVE ASSESSMENT

The objective of comprehensive assessment is to capture the overall costs associated with an intelligence program in order to inform the debate between security and liberty. It attempts to answer the questions: what are the privacy costs and are these costs acceptable? Based on the results of the primary assessment, the comprehensive analysis contextualizes the overall concerns raised by a program, identifies any deficiencies in the program, and assesses what has the most negative effect on the overall privacy costs. For example, if the intelligence program's only source of information derives from First Amendment protected activities, there are no other privacy concerns implicated, and all the safeguards are in place except for Congressional and Judicial oversight the comprehensive assessment would be as follows. In this example, the overall concerns are related to the privacy factors with the most negative effect: the Executive branch would be unchecked by other branches of the government while it infringed on the privacy of Americans participating in free speech, religion, or political expression. The significant shortfall would be the lack of Congressional and Judicial oversight. The

158 This figure uses the information about FBI surveillance programs detailed in Chapter II.

comprehensive assessment provides this level of analysis to the overall privacy costs (Figure 6).

Comprehensive Assessment	
Overall Concerns:	While this program does not invoke many of the privacy concerns and has numerous safeguards, the particular combination of targeting First Amendment protected activities without Congressional or Judicial oversight is troublesome.
Shortfalls:	Lack of Congressional and Judicial oversight
Most Negative Effect:	Executive branch would be unchecked by other branches of the government while it infringed on the privacy of Americans exercising free speech, religion, or political expression

Figure 6. Example Comprehensive Assessment

Acceptability, the second element that the comprehensive analysis addresses, is not a normative judgment about the ultimate costs associated with an intelligence program. Instead, it is a subjective representation of the public's tolerance for intelligence tools, lack of safeguards, or the reach of a program. Acceptability contextualizes a program's privacy concerns by indicating which concerns are higher priorities or where the scope of the program falls in relation to public tolerance. Determining a subjective acceptance level requires comparing the scope of the intelligence program—measured in both the number of total people affected and the number of Americans affected—with public opinion. For example, the TIA program would have had unlimited access to credit card transactions, which would have affected every American with a credit card at the time.[159] Would the government collecting and accessing data on the credit card transactions of over 159 million Americans[160] have been within the threshold of public tolerance in 2002? According to public opinion in 2002, 43 percent of Americans approved of the government accessing credit card records.[161] The percentage of Americans that would have been affected, however, would have been higher than the percentage of those who approved (Figure 7). Consequently, the scope of the program

159 The TIA capabilities are detailed in Chapter II.

160 U.S. Department of Commerce, Bureau of the Census, *Statistical Abstract of the United States, 2012* (Washington, DC: Government Printing Office, 2012), table 1188.

161 "Balancing Act: National Security and Civil Liberties in Post-9/11 Era," Carroll Doherty, Pew Research Center, June 7, 2013, http://www.pewresearch.org/fact-tank/2013/06/07/balancing-act-national-security-and-civil-liberties-in-post-911-era/.

would have been subjectively unacceptable, thus increasing the privacy costs. Although public opinion is not an authoritative gauge for the acceptability of an intelligence program, it nonetheless puts the concerns into context—which either subjectively increases or decreases the privacy costs.

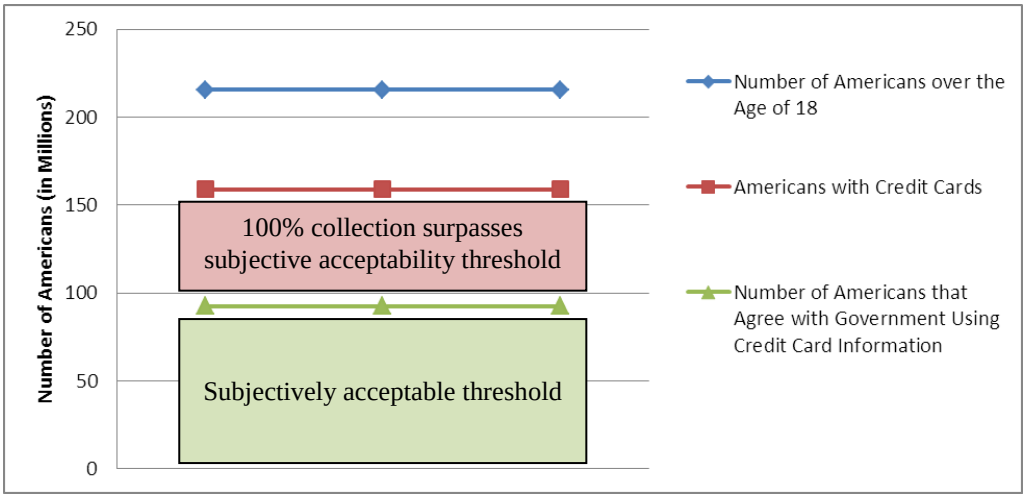

Figure 7. Example of Acceptability Analysis[162]

C. CONCLUSION

Measuring privacy costs requires a primary analysis that determines whether a certain privacy concern applies to an intelligence program and then assesses a positive or negative privacy cost. The comprehensive assessment builds off the primary evaluation and determines what the overall costs are for a given program. This requires an examination of the cumulative results of the primary analysis to identify the overall concerns raised by a program, its shortfalls, and which areas have the most negative effects on the program's privacy costs. The comprehensive assessment also addresses the acceptability of the privacy concerns, which puts the overall costs into context.

There are limitations to measuring privacy costs. Alternative options such as a scoring system would be insufficient because measuring privacy costs is not amenable to

[162] Ibid.; Bureau of the Census, *Statistical Abstract*, table 1188; Bureau of the Census, *Population Estimates: Annual Resident Population Estimates of the United States by Age and Sex* (Washington, DC: Government Printing Office, 2002).

quantitative analysis. Assigning numerical values to privacy concerns runs the risk of devaluing legitimate privacy interests. That an American has a subjective and reasonable expectation of privacy is just as valid of an interest as the right to participate in First Amendment protected activities free from government surveillance. One concern should not be valued more than the other; the real value is simply that a privacy concern exists. Moreover, safeguards can minimize risks, but these cannot negate the presence of a legitimate privacy concern. That an analyst does not know to whom the information pertains because it is anonymous does not annul the privacy concern created by the government collecting personal information. The purpose of measuring privacy costs is to inform what is at stake; it is not the role of arbitrary numbers to determine what is a high, low, or worthwhile privacy cost. That decision is left to society as it balances between security and liberty.

D. PRIVACY COSTS ASSESSEMENT FORM

Primary Assessment			
Privacy Concerns	**Yes or No**	**Privacy Safeguards**	**Yes or No**
Program collects or accesses personal information:	Yes: Supports valid privacy interest and increased privacy cost	Parties responsible conducted a privacy impact assessment:	Yes = Mitigates privacy concerns and decreases privacy cost
Information collected or accessed is being used for other than intended purpose:	No: Does not support the presence of a valid privacy interest	Sharing of intelligence products derived from personal information is limited:	No = Increases privacy concerns and increases privacy cost
Information falls under a subjective expectation of privacy:		Access to personal information is restricted:	
Society recognizes the expectation of privacy as reasonable:		Program is subject to Executive oversight:	
Information collected or accessed is derived from activities protected under the First Amendment:		Program is subject to Congressional oversight:	
		Program is subject to Judicial oversight:	
		Accountability mechanisms enable the auditing of access to and use of personal information:	
		The information is made anonymous:	
Comprehensive Assessment			
Overall Concerns:			
Shortfalls:			
Most Negative Effect:			
Indicators of Acceptability			

Figure 8. Privacy Costs Assessment Form

THIS PAGE INTENTIONALLY LEFT BLANK

V. MEASURING PRIVACY COSTS OF A MODERN INTELLIGENCE PROGRAM

One of the most controversial domestic surveillance programs in modern times is an NSA program that collects business record (BR) metadata in bulk under Section 215 authorities of the Patriot Act.[163] A vast majority of these records pertains to communications of U.S. persons within the United States.[164] The NSA BR metadata program has consequently received heavy criticism for infringing on Americans' privacy, which has generated numerous calls for reform by some members of Congress and the public. On the other side of the issue are people who argue that the program is an effective counterterrorism tool. The debate is essentially between security and liberty, but that conversation is uninformed until those involved know what the privacy costs are. This chapter will take the method for measuring privacy costs outlined in Chapter IV and apply it to the NSA BR metadata program. A majority of the chapter will focus on the primary and comprehensive assessments of the overall privacy costs. It will conclude with an evaluation of recent changes to intelligence practices and determine what effect these reforms will have on the privacy costs associated with the BR metadata program.

A. PRIMARY ASSESSMENT

1. Privacy Concerns

This section will measure the privacy concerns of the BR metadata program in accordance with the method established in Chapter IV. Specifically, it will determine if the program uses information for other than its originally intended purpose, uses personal information, infringes on an expectation of privacy, or targets First Amendment protected activities.

---

163 U.S. Department of Justice, Office of Intelligence, National Security Division (NSD), *Report on the National Security Agency's Bulk Collection Programs Affected by USA PATRIOT Reauthorization*, February 2, 2011,1; NSD, *Report on the National Security Agency's Bulk Collection Programs Affected by USA PATRIOT Reauthorization*, December 14, 2009, 3.

164 Foreign Intelligence Surveillance Court (FISC), *Supplemental Opinion and Order*, Docket Number: BR 09-15, November 5, 2009, 5.

a. Using Information for Another Purpose

The first question to answer is: does the NSA BR program use information for something other than the original purpose of that information? Under the BR program, the NSA collects bulk metadata from U.S. telecommunications providers.[165] It obtain this information from telecommunications companies by providing a court order that requires them to produce business records on nearly all the telephone calls each one handles both in and out of the country as well as calls made entirely within the United States.[166] It then uses this information to conduct call chaining, which is a form of intelligence analysis.[167] Thus, the program takes information from telecommunication companies originally intended for the limited purposes of establishing a contractual relationship and maintaining billing records and uses it to analyze a person's communication habits and contacts. The BR program clearly uses metadata for a purpose other than those the companies and customers originally intended.

b. Personal Information

The second question to answer is: does the NSA BR program collect or access personal information? This question is difficult to answer. On the one hand, the data is intentionally stripped of personal information. It does not collect the content of communications or the name, address, or financial information of a subscriber.[168] Instead, the BR program collects the following types of information:[169]

- Telephone numbers
- Times of communication
- Dates of communication

---

165 NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2009, 2.

166 Ibid., 3.

167 NSD, *Memorandum of the United States in Response to the Court's Order Dated January 28, 2009*, Docket Number: BR 08-13, February 17, 2009, 3.

168 NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2009, 3,5; NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2011, 5; FISC, *Primary Order*, Docket Number: BR 13-80, April 25, 2013, 3; FISC, *Order*, Docket Number: BR 06-05, May 24, 2006, 2.

169 NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2009, 3,5; NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2011, 5; FISC, *Primary Order*, BR 13-80, 2013, 3; FISC, *Order*, BR 06-05, 2006, 2.

- Duration of a call
- International Mobile Subscriber Identity (IMSI) number
- International Mobile station Equipment Identity (IMEI) number
- Trunk identifier
- Telephone calling card numbers

While this data can be quite revealing, without the identifying information it only depicts activities of a nonspecific person.

On the other hand, the NSA analysis of the metadata is supposed to identify terrorists. The BR program is misleading in this regard because its purpose is to uncover the tactics used by terrorist organizations to disguise and obscure their identities.[170] Thus, if the program is successful, then it can learn these tactics and potentially reverse them to identify terrorists. After all, that is what the program is designed to do: "analysis of the BR metadata addresses a critical, threshold issue for the Government's efforts to detect and prevent terrorist acts affecting the national security of the United States: identifying the terrorists and their associates."[171] This stated objective, however, is how the BR program fits into overall counterterrorism efforts. The actual purpose of the BR program is to determine if terrorist networks are communicating with anyone inside the United States, but the identification process stops at the telephone identifier without accessing any personal information.[172] Subsequent actions might access personal information to identify who is using the telephone that is communicating with terrorists, but that is not done by the NSA—it is done by the FBI (more on the NSA and FBI coordination will be addressed in the Limited Dissemination part of the Privacy Safeguards section). The data collected and accessed under the NSA BR program treads a fine line between ambiguous and personal information. Without any identifiable information to tie the metadata back to, however, the NSA program does not invoke privacy concerns associated with personal information.

---

170 FISC, *Order*, Docket Number: BR 08-13, March 2, 2009, 2.

171 NSD, *Report of the United States*, Docket Number: BR 09-09, August 17, 2009, 50.

172 Ibid., 50–51.

c. Subjective and Reasonable Expectation of Privacy

Do Americans have a subjective expectation of privacy over their phone records and is society willing to recognize that expectation as reasonable? The Office of the Director of National Intelligence (ODNI) General Counsel Robert Litt argued that according to the third party doctrine, Americans do not have a legally valid expectation of privacy over the BR metadata.[173] At the same time, Litt recognized that changing technology is influencing privacy interests; Americans are giving away "massive amount of information" about themselves.[174] An important distinction is that Americans are not giving their information to the government. Litt specifically commented on how Americans provide their information to private companies but do not want the government to have this information.[175] According to the subjective and reasonable standards applied in this thesis, that point demonstrates intent by the American people to restrict the sharing of that information with the government. Thus, a person entering into a contract with a telephone company chooses to provide limited information to that company and not to the government, thereby exhibiting a subjective expectation of privacy. This expectation is also reasonable from a societal perspective because having a telephone is part of normal life, communicating is a routine social interaction, phones are the technology over which it occurs, and providing information to a company does not equate to consent for government surveillance. Americans have an expectation of privacy over BR metadata.

d. First Amendment Protected Activities

The final question to answer is: does the BR program collect or access information created during First Amendment protected activities? The answer is no. While the metadata pertains to communications, which someone could argue is protected

---

173 Robert S. Litt, *Privacy, Technology and National Security: An Overview of Intelligence Collection*, Office of the Director of National Intelligence, (ODNI), July 19, 2013, 2, http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection?tmpl=component&format=pdf.

174 Ibid., 3.

175 Ibid., 4.

under First Amendment freedom of speech, the program does not collect content.[176] Thus, the protected activity—speech—is not the source of information. Additionally, there are forceful restrictions that prevent the BR program from infringing on First Amendment protections. For example, the government cannot determine that a U.S. person is associated with an international terrorist organization solely based on his or her First Amendment activities.[177] Collecting the BR metadata must be relevant to an authorized investigation,[178] and that investigation of potential ties between a U.S. person and an international terrorist organization cannot solely be based on First Amendment protected activities.[179] Thus, even though speech, religion, and political expression fall dually within the characteristics of terrorism and First Amendment freedoms, these activities are protected. An association with terrorism has to exist in order for the government to investigate, collect, and subsequently use the metadata. Consequently, there is no First Amendment privacy concern in the NSA BR program.

2. Privacy Safeguards

This section will apply the method established in Chapter IV to determine what safeguards the BR program institutes to mitigate privacy concerns. It will evaluate the following tools and procedures: privacy impact assessment, limitations on dissemination, restrictions on access, executive, congressional, and judicial oversight, and mechanisms that enable auditing and make the information anonymous.

a. Privacy Impact Assessment

There is no indication that the government conducted a PIA for the BR metadata program. None of the declassified documents by ODNI have yet to include a PIA.[180]

---

176 NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2009, 3,5; NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2011, 5; FISC, *Primary Order*, BR 13-80, 2013, 3; FISC, *Order*, BR 06-05, 2006, 2.

177 FISC, *Primary Order*, Docket Number: BR 09-13, September 3, 2009, 8.

178 FISC, *Primary Order*, BR 13-80, 2013, 2.

179 Ibid., 2; FISC, *Primary Order*, BR 09-13, 2009, 8.

180 The declassified documents are announced and posted on "Press Releases," Office of the Director of National Intelligence, http://www.dni.gov/index.php/newsroom/press-releases. As of February 28, 2014, there has been no release pertaining to a PIA of the NSA BR metadata program under Section 215 of FISA.

While the evidence is inconclusive, it is likely that the government never conducted a PIA because of how the program developed. In the immediate aftermath of 9/11, President Bush used Executive authority to sanction the collection of telephone metadata, which Congress subsequently codified into law.[181] Thus, out of emergent circumstances the program emerged and then continued to expand to what it is today.

b. Limited Dissemination

One of the most basic privacy safeguards is to limit how much of the metadata is shared throughout the intelligence community. The BR program limits dissemination in two ways: internally and externally. Only analysts in the NSA trained in specific handling, dissemination, and usage guidelines can see BR metadata query results before the information is minimized.[182] The minimization process governs the collection, processing, retention, and dissemination of information about U.S. persons.[183] For example, instead of using a name, intelligence can use the term U.S. person.[184] What this means in context to the BR program is that before any of the approved analysts shares the intelligence with anyone else, they must first transform some of the data into general information that protects against the possibility of anyone determining to whom the information refers. For external dissemination, NSA must also minimize the results of metadata queries.[185] NSA applies such a strict interpretation of minimization it prohibits the sharing of the telephone number because someone can use it to identify who the person is. The result might be an intelligence report that warns of Al-Qaeda communicating with several U.S. persons within the United States at a higher frequency than normal without specifying what telephone numbers it is calling.

---

[181] ODNI, "DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001," press release, December 21, 2013, http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/991-dni-announces-the-declassification-of-the-exisitence-of-collection-activities-authorized-by-president-george-w-bush-shortly-after-the-attacks-of-september-11,-2001.

[182] FISC, *Primary Order*, BR 13-80, 2013, 12–13.

[183] NSA, *U.S. Signals Intelligence Directive 18: Legal Compliance and Minimization Procedures*, revised January 25, 2011, 41–50.

[184] Ibid., 48.

[185] FISC, *Primary Order*, BR 13-80, 2013, 13.

Exceptions to the minimization rule can occur if specific criteria are met.[186] The NSA cannot disseminate un-minimized information about a U.S. person unless it is necessary to understand the value of the foreign intelligence, it is evidence of a crime, or it "indicates a threat of death or serious bodily harm."[187] Yet even in these circumstances, the FBI must follow additional minimization procedures for domestic operations after it receives the intelligence from NSA.[188] These exceptions are also rare. Despite collecting a considerable amount of metadata, the NSA only provides an average of two telephone numbers per day to the FBI.[189] Overall, the most personal information shared by the BR program is a very small amount of telephone numbers linked to international terrorist organizations.

c. Restricted Access

While the BR program collects an immense amount of data, the NSA tightly restricts access to the metadata. The only government agency that stores and accesses the information is the NSA.[190] It restricts access by applying unique markings to the metadata so that software can control who queries the data.[191] Only those at the NSA with authorization and specific training can access the information and only for specific purposes.[192] First, there must be a reasonable, articulable suspicion (RAS) that the telephone number is associated with a terrorist organization on an official government list in order for an analyst to query the database.[193] Second, a query requires an approved telephone number as the search term and only for the purpose of call chain analysis.[194]

---

186 Ibid., 13.

187 ODNI, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, June 8, 2013, 2. http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/871-facts-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act

188 FISC, *Primary Order*, BR 13-80, 2013, 4; FISC, *Order*, BR 06-05, 2006, 4.

189 FISC, *Order*, BR 06-05, 2006, 4.

190 FISC, *Primary Order*, BR 13-80, 2013, 4.

191 Ibid., 4–5.

192 Ibid., 5: FISC, *Order*, BR 06-05, 2006, 5.

193 NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2009, 4.

194 FISC, *Primary Order*, BR 13-80, 2013, 6–7.

Most of these telephone numbers are on an alert list reviewed and authorized by the FISC,[195] but a select group of twenty-two officials can approve a number if there is RAS that it connects to one of the listed terrorist organization.[196] Thus, it is only when an approved telephone number is associated with an international terrorist organization that one of the few authorized and trained analysts can access BR metadata. As of 2008, the FISC limited that number to a mere 85 analysts.[197] Access to the data is clearly restricted.

d. Executive Oversight

The DOJ, ODNI, and NSA mainly handle oversight of the BR program. The coordination and reporting requirements for Executive oversight is extensive. As mentioned above, the collection of BR metadata occurs by serving a court order to the telecommunications companies. That order is generally effective for 90 days. During that period, the following types of oversight occur. First, representative from the NSA Office of General Council (OGC), Office of the Director of Compliance, and DOJ review the program's compliance with the FISC order and submit their findings in writing to the court.[198] Second, every 90 days DOJ must review a sample of the queries made against the BR metadata.[199] Third, every 45 days the OGC reports to the Director on the effectiveness of NSA's oversight of data on U.S. persons.[200] Fourth, twice during the authorized period of collection the National Security Division (NSD) of DOJ reviews both the NSA's justifications for approving telephone identifiers as well as the queries conducted against the BR metadata.[201] Every 36 days the NSA must file a report with

195 Ibid., 9.

196 Ibid., 7,10.

197 FISC, *Order*, BR 08-13, 2009, 9.

198 FISC, *Primary Order*, BR 13-80, 2013, 15; FISC, *Primary Order*, BR 09-13, 2009, 17.

199 FISC, *Order*, BR 06-05, 2006, 8.

200 Ibid., 8.

201 FISC, *Primary Order*, BR 09-13, 2009, 16.

the court that accounts for all dissemination of U.S. person data in any form outside the NSA that occurred since the last report.[202]

An obvious criticism is that since the same branch of government running a secret program is also reviewing its compliance with legal requirements, the oversight is likely just a rubber stamp. The available record, however, indicates otherwise. For examples, when a DOJ and NSA review discovered a compliance issue they immediately informed the FISC as well as the intelligence committees in Congress and the Director of NSA initiated a comprehensive review of the program.[203] The problems generally related to a few instances where unauthorized NSA analysts received un-minimized BR metadata reports and technical issues that resulted in broad the dissemination of similar information.[204] The causes of the compliance issues were related to technical errors in the software and operator mistakes,[205] but these were subsequently remedied. The self-identification of the compliance problem and immediate reporting of the issues to the other oversight bodies demonstrates a persistent Executive oversight program.

e. Congressional Oversight

Members of the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) have stated that they were aware of the BR program.[206] Not only were the committee members aware, but so were other members of Congress.[207] The Executive branch also claimed to regularly inform Congress, which is supported by declassified letters from the DOJ to the SSCI and

---

202 FISC, *Primary Order*, BR 13-80, 2013, 16.

203 NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2009, 4.

204 Ibid., 4.

205 Ibid., 4; NSD, *Report of the United States*, BR 09-09, 2009, 57.

206 Parmy Olson, "U.S. Senators: NSA Cellphone Spying Has Gone On 'For Years,'" *Forbes*, June 6, 2013, http://www.forbes.com/sites/parmyolson/2013/06/06/u-s-senators-nsa-cellphone-spying-has-gone-on-for-years/; Glenn Kessler, "Obama's Claim that 'Every Member of Congress' Was Briefed on Telephone Surveillance," *The Fact Checker* (blog), *Washington Post*, June 11, 2013, http://www.washingtonpost.com/blogs/fact-checker/post/obamas-claim-that-every-member-of-congress-was-briefed-on-telephone-surveillance/2013/06/10/fd03ea8e-d21f-11e2-8cbe-1bcbee06f8f8_blog.html; Imtiyaz Delawala, "Intelligence Committee Leaders Defend NSA Surveillance," *ABC News*, June 9, 2013, http://abcnews.go.com/blogs/politics/2013/06/intelligence-committee-leaders-defend-nsa-surveillance/.

207 Olson, "U.S. Senators"; Kessler, "Obama's Claim that 'Every Member of Congress.'"

HPSCI about the BR metadata program.[208] The DOJ also provides annual reports to the SSCI and HPSCI on the BR metadata program.[209] Moreover, Congress extended the powers of the surveillance program under the FISA Amendments Act of 2008 and reauthorized these authorities in 2012.[210] While there may have been disagreements regarding the BR metadata program, Congress was informed and made decisions that affected the program. It conducted oversight.

f. Judicial Oversight

The FISC has the authority to determine and enforce the BR metadata program's compliance with its orders and the law.[211] At times, this oversight is administrative in nature such as when it reviews the NSA, DOJ, and ODNI reports or approves telephone numbers that can be used to access the BR metadata.[212] Other times, the oversight is fierce. For example, although the FISC determined that there were no intentional or bad-faith violations of its orders during the compliance issues,[213] it nonetheless held the NSA accountable for the problems. At one point, the FISC ordered the government to complete and provide the results of an end-to-end system review of the program, provide an affidavit that describes the value of the metadata to national security, demonstrate that the metadata are for authorized investigations, submit an affidavit stating that the technological remedies have been tested and are successful, and explain additional

---

208 NSD, *The Attorney General's Annual Report on Access to Certain Business Records for Foreign Intelligence Purposes Under the Foreign Intelligence Surveillance Act*, April 2011; NSD, *The Attorney General's Annual Report on Access to Certain Business Records for Foreign Intelligence Purposes Under the Foreign Intelligence Surveillance Act*, April 2012.

209 NSD, *Report on the National Security Agency's Bulk Collection Programs* 2009, 4; NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2011, 4; ODNI, *Facts on the Collection of Intelligence*, 1–2; ODNI, "DNI Clapper Declassified Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)," press release, September 10, 2013; http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document.

210 FISA Amendments Act of 2008, Public Law 110-261, 110th Cong., July 10, 2008; FISA Amendments Act Reauthorization Act of 2012, Public Law 112-238, 112th Cong., December 30, 2012.

211 FISC, *Order*, BR 08-13, 2009, 14.

212 NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2009, 4; FISC, *Primary Order*, BR 13-80, 2013, 9,15.

213 NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2009, 4.

remedial steps the government will take.[214] The court required these steps to restore its confidence in the government's ability to protect information about U.S. persons. Until this occurred, the FISC approved BR metadata collection on a case-by-case basis instead of the usual bulk method.[215] The FISC also ordered the government to explain the compliance incidents in full and provide supporting documentation so the court can determine if it should modify or rescind the order, direct additional remedial steps, or take legal action against the people responsible for the misrepresentations or violations of the order.[216] These examples demonstrate that not only is there Judicial oversight of the BR metadata program, but that role provides an important safeguard against the privacy concerns inherent in the program.

g. Auditing Access to Personal Information

Under the BR metadata program, any of the metadata that concerns a U.S. person is "subject to strict and frequent audit and reporting requirements."[217] For example, every time that an unapproved telephone number is used to query the metadata, a record is generated.[218] In addition, every time someone accesses the metadata, the system automatically creates an auditable record that includes the user's login identifier, IP address from which the request generated, date and time of the query, and the specific search request.[219] Thus, there is strict auditing of who accesses the metadata and how it is used, the results of which are included in the Executive and Judicial oversight reports.[220]

---

214 FISC, *Order*, BR 08-13, 2009,19–20.

215 Ibid., 12–18; ODNI, "DNI Clapper Declassified Intelligence Community Documents."

216 FISC, *Order Regarding Preliminary Notice of Compliance Incident Dated January 15, 2009*, Docket Number: BR 08-13, January 28, 2009, 2.

217 NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2009, 2; NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2011, 5.

218 FISC, *Primary Order*, BR 13-80, 2013, 7.

219 FISC, *Order*, BR 06-05, 2006, 6; FISC, *Primary Order*, BR 09-13, 2009, 12.

220 NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2009, 2; NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2011, 5; FISC, *Order*, Docket Number: BR 09-06, June 22, 2009, 7.

h. Information Is Anonymous

The information is anonymous at collection because of the prohibition on collecting names or addresses.[221] Additionally, the telephone number is treated as personal information and is protected as such. Even if a telephone number belonging to a U.S. person is affiliated with an international terrorist organization, that telephone number is still treated in accordance with the minimization procedures that protect the personal information of U.S. persons.[222] The BR metadata is anonymous information.

B. COMPREHENSIVE ASSESSMENT

The next step in the measuring process contextualizes the overall concerns raised by the BR program, identifies any deficiencies in the safeguards, and assesses what has the most negative impact on the overall privacy costs. This comprehensive assessment will attempt to answer the questions: what are the privacy costs and are these costs acceptable? The overall privacy concern is that the BR metadata program collects substantial amounts of data on Americans that falls under an expectation of privacy. While there are strong safeguards in place to protect against abuses, the primary shortfall is that no PIA was conducted. In order to be most effective, safeguards must address anticipated privacy issues. Without a PIA, however, there was insufficient insight into what these problems could be and, consequently, many issues that could have possibly been addressed at the outset of the program were not. Without a PIA, there is an increased chance that privacy problems will arise. The compliance issues with the BR metadata program thus far have proven this negative effect to be true. Example problems include analysts being able to query the data without a RAS-approved telephone number, a software tool could override the limit on how many numbers the call chain analysis could search, and the CIA, FBI, and National Counterterrorism Center (NCTC) could

---

[221] NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2009, 3,5; NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2011, 5; FISC, *Primary Order*, BR 13-80, 2013, 3; FISC, *Order*, BR 06-05, 2006, 2.

[222] FISC, *Primary Order*, 13-80, 2013, 13; NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2009, 2; NSD, *Report on the National Security Agency's Bulk Collection Programs*, 2011, 5; FISC, *Order*, BR 06-05, 2006, 6.

access un-minimized information about U.S. persons.[223] A PIA could have potentially identified these problem areas and the government could have implemented safeguards before the compliance issues occurred.

A vast majority of the BR metadata the NSA collects is irrelevant to FBI investigations yet pertains to the communications of U.S. persons within the United States.[224] Does this practice fall within the tolerance of the American people? To assess whether or not the program is acceptable requires a comparison of the scope of collection, access, and use of the information with public opinion. There is no publicly available information on how much of the U.S. person metadata the NSA accesses. There is, however, information related to the scope of collection and the use of metadata.

There is no escaping that the amount of metadata collected under the BR program is substantial. As of 2014, the number of American adults with cell phones was at 91 percent of the population.[225] If the NSA collected against every device in the United States, the program would affect 223 million American adults.[226] Due to capability limitations, the recent scope of collection turns out to be much less than complete coverage. According to multiple reports, the NSA is only collecting between 20 and 30 percent of the overall call records in the United States.[227] Americans own more than one device on average, which means 20 to 30 percent of call records affects between roughly 45 and 68 million Americans.[228] Back to the original question of acceptability, where do

---

223 NSD, *Report of the United States*, BR 09-09, 2009, 56–58; Litt, *Privacy, Technology and National Security*, 1.

224 FISC, *Supplemental Opinion*, BR 09-15, 2009, 5.

225 "Mobile Technology Fact Sheet," Pew Research Center, December 27, 2013, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.

226 Bureau of the Census, *National Population Projections, 2008* (Washington, DC: Government Printing Office, 2012), table 2.

227 Ellen Nakashima, "NSA Is Collecting Less than 30 Percent of U.S. Call Data, Officials Say," *Washington Post*, accessed March 5, 2014, http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html; Siobhan Gorman, "NSA Collects 20% or Less of U.S. Call Data," *Wall Street Journal*, February 7, 2014, http://online.wsj.com/news/articles/SB10001424052702304680904579368831632834004.

228 "Global Mobile Statistics 2013 Part A: Mobile subscribers; handset market share; mobile operators," mobiThinking, June 2013, http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#uniquesubscribers; Bureau of the Census, *National Population Projections*, table 2.

these collection numbers fall in relation to the public's tolerance of the NSA program? The most recent number that specifically measures the acceptability of telephone tracking shows that 56 percent of the population approve of the intelligence method.[229] If the government collected all phone data, it would clearly be beyond the threshold of the American public (Figure 9). At a decreased capacity, however, it could be tolerable if the limited scope was intentional. Being that the decreased collection is due to technical limitations and not an inherent restriction on the BR program, the intended scope of the metadata collection is beyond public tolerance and therefore increases the subjective privacy concerns associated with the program.

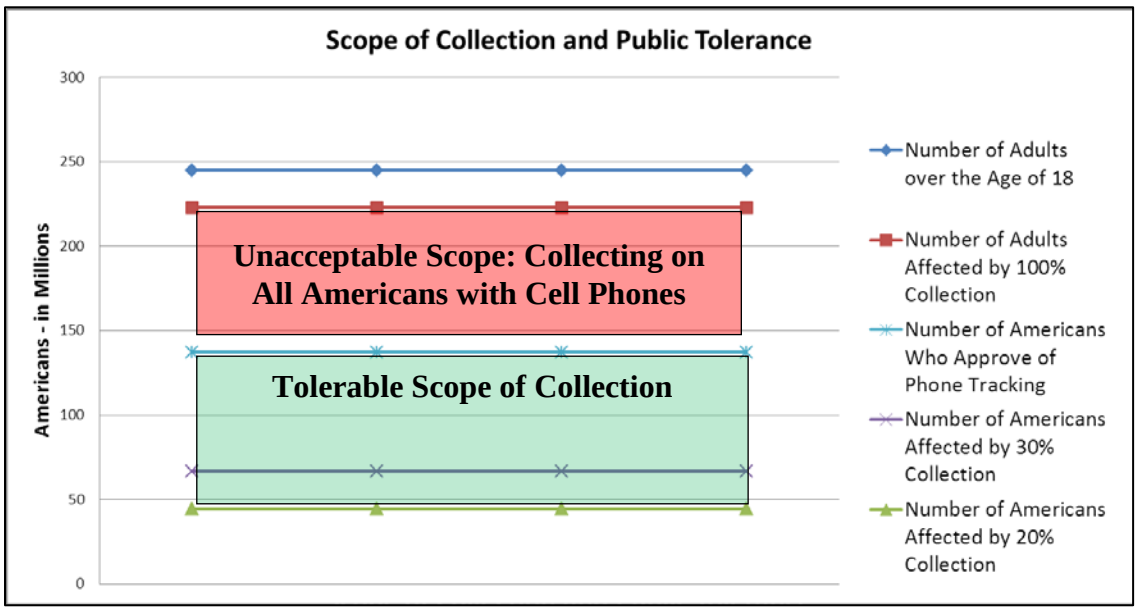

Figure 9. Scope of Collection and Public Tolerance

How much metadata the government uses provides a different conclusion about acceptability. The usage numbers are miniscule. Between 2006 and 2009, the NSA provided the FBI with an average of 853 telephone numbers per year.[230] While the program accessed more numbers through call chaining, usage is limited to the amount of

229 "Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic," Pew Research Center, June 10, 2013, http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/.

230 FISC, *Order*, BR 08-13, 2009, 13.

telephone numbers passed to the FBI for a counterterrorism investigation. In essence, the comparison is between how many Americans the government collects on and how many of these Americans it investigates under the authority to prosecute. If the NSA collected on every American with a cell phone, only 0.00026 percent of these people would have their number passed to the FBI. If the NSA were collecting the lesser 30 percent of calling data, then it would still only affect 0.00085 percent of the people. This is well below the public tolerance reflected in public opinion (Figure 10). Moreover, since the telephone numbers investigated and passed on to the FBI are reasonably believe to be associated with a known terrorist organization, the chances that a law abiding citizen's telephone number is affected is even less. The amount of telephone numbers used by the government is subjectively acceptable. Consequently, the overall subjective analysis reveals that scope is well beyond public tolerance but the extremely limited amount of metadata used by the government is within the acceptable range, so long as the safeguards for access and dissemination are effective.

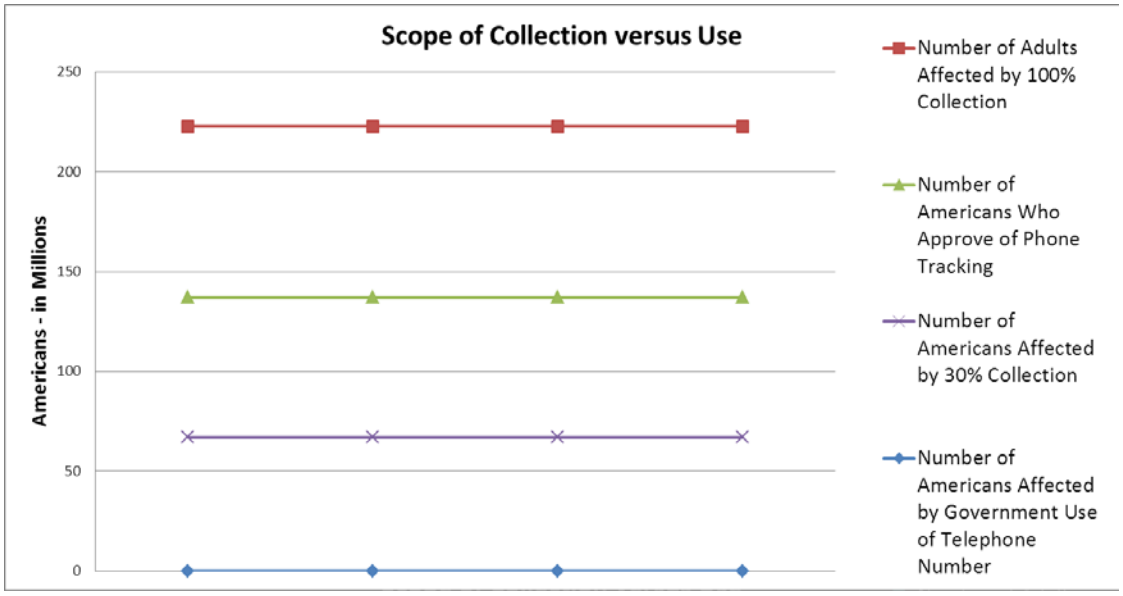

Figure 10. Scope of Collection versus Use

C. CHANGES TO THE BR METADATA PROGRAM

In January 2014, President Obama announced several changes to intelligence programs, which specifically included the NSA BR metadata program.[231] The purpose of the reforms is to better protect privacy without degrading the effectiveness intelligence.[232] In order to accomplish this, however, the changes would need to address the issues raised in this chapter. It is therefore informative to review what effect, if any, there will be on the BR metadata privacy concerns and safeguards.

The new Presidential Policy Directive-28 (PPD-28) established new limits on the use of SIGINT that is collected in bulk, but the approved list of justifications includes the terrorism nexus originally required in the BR program.[233] Similarly, the dissemination, retention, access, and oversight requirements in PPD-28 do not change the BR metadata safeguards already in-place for information related to U.S. persons.[234] The scope of collection will also effectively be the same. While the reforms call for external storage of the BR metadata outside of the government's control,[235] collecting the data will still be in bulk and pursuant to FISC orders based on an authorized investigation, which is how the program already operates.[236]

The new requirements do create additional restrictions on access. Through a software program, contact chaining can access a U.S. person's metadata even if an NSA analyst never sees that U.S. person's telephone number. Previously, the program was permitted to pursue telephone identifiers three steps removed from the one used to search

---

231 White House, Office of the Press Secretary, "FACT SHEET: Review of U.S. Signals Intelligence," news release, January 17, 2014, http://www.whitehouse.gov/the-press-office/2014/01/17/fact-sheet-review-us-signals-intelligence.

232 Ibid.

233 Barrack Obama, Presidential Policy Directive (PPD)-28, "Signals Intelligence Activities," January 17, 2014, 3–4.

234 Ibid., 5–6.

235 Office of the Press Secretary, "FACT SHEET."

236 Office of the Press Secretary, "Remarks by the President on Review of Signals Intelligence," news release, January 17, 2014, http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

the data, but the reforms decrease the threshold to two steps removed.[237] Tighter access restrictions, however, were not a major problem with the BR metadata program. Thus, while it does improve a privacy safeguard, the change is unsubstantial. The reforms also seek to establish a body of independent advocates to participate in significant FISC cases,[238] but the outcome is the same as that for improving limitations on access: the effect on privacy costs may very well be beneficial, but it does not address the core privacy issues in the BR program.

Interestingly, the President's Review Group on Intelligence and Communications Technologies provided a recommendation that would have addressed the major privacy concerns of the BR metadata program. Tasked with surveying the broad intelligence apparatus of the U.S. government and to recommend changes, the group specifically stated that the government should conduct privacy and civil liberties impact assessments not just on future programs, but on those currently in existence.[239] There is yet to be any indication that the government will conduct a PIA of the BR metadata program. Consequently, new and old safeguards will continue to respond to infringements instead of preempting privacy violations by focusing efforts on identifiable areas of concern. In effect, that is what is occurring through this iteration of reforms. While the intention to protect privacy is genuine, these changes will not decrease the privacy costs associated with the BR program.

---

[237] Office of the Press Secretary, "FACT SHEET."

[238] Office of the Press Secretary, "Remarks by the President."

[239] The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, December 12, 2013, 38–39.

NSA BR Metadata Program			
Primary Assessment			
Privacy Concerns	**Yes or No**	**Privacy Safeguards**	**Yes or No**
Program collects or accesses personal information:	No	Parties responsible conducted a Privacy Impact Assessment:	No
Information collected or accessed is being used for other than intended purpose:	Yes	Intelligence products derived from personal information is restricted:	Yes
Information falls under a subjective expectation of privacy:	Yes	Access to personal information is limited:	Yes
Society recognizes the expectation of privacy as reasonable:	Yes	Program is subject to Executive oversight:	Yes
Information collected or accessed is derived from activities protected under the First Amendment:	No	Program is subject to Congressional oversight:	Yes
		Program is subject to Judicial oversight:	Yes
		Accountability mechanisms enable the auditing of access to and use of personal information:	Yes
		The information is made anonymous:	Yes
Comprehensive Assessment			
Overall Concerns:	The BR program collects substantial amounts of data that are under an expectation of privacy.		
Shortfalls:	The primary shortfall is that there is no indication the government conducted a Privacy Impact Assessment (PIA).		
Most Negative Effect:	The absence of a PIA has a substantial negative effect. Other safeguards respond to privacy issues as they occur, but with a PIA many issues can be understood and resolved prior to the occurrence of a violation. Consequently, without the PIA there is an increased chance that privacy problems will arise.		

Figure 11. Privacy Costs of BR Metadata Program-Part 1

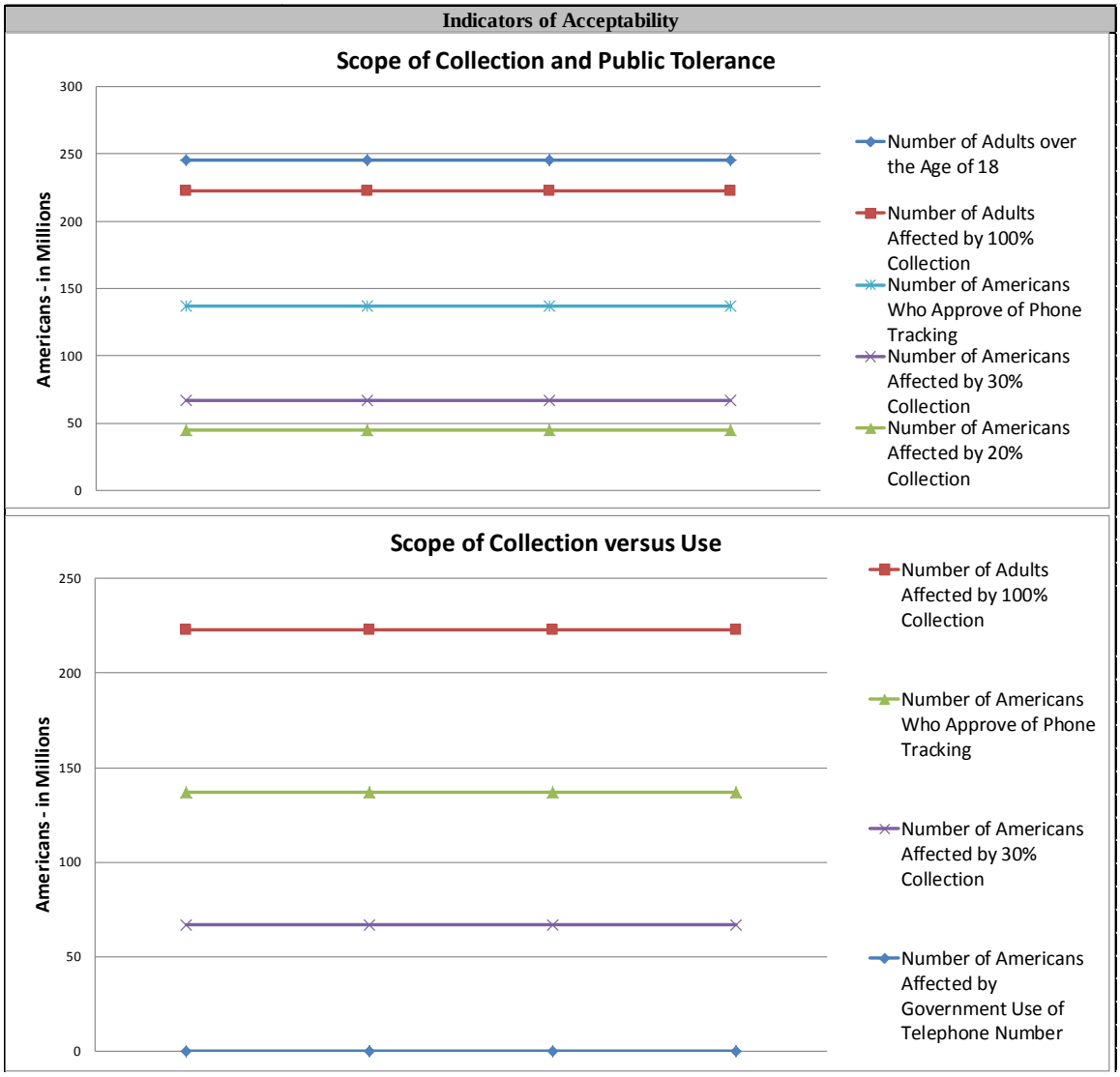

Figure 12. Privacy Costs of BR Metadata Program-Part 2

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND IMPLICATIONS

A. SYNOPSIS

Chapter I laid out the core arguments in the security versus liberty debate and identified the shortcomings with each. Even for the most practical approach, the balancing act, there was a fundamental flaw: we could measure the security side of the scale, but lacked any meaningful framework to measure the costs to privacy, which represents the liberty side of the scale. The chapter proposed two issues to investigate in order to identify key indicators for measuring privacy costs. First was the expectation Americans have for government behavior in domestic intelligence programs, which the thesis addressed in Chapter II. Second was the expectation Americans have for privacy discussed in Chapter III.

Chapter II conducted an historical and comparative analysis of Cold War-era domestic surveillance programs and the Pentagon's attempt at TIA in the aftermath of 9/11. Both of these cases were quite informative about what Americans expect for government behavior. The analysis in Chapter II identified the following key elements for measuring privacy costs:

- Does the program collect or access personal information?
- Is the collected or accessed information used for other than the originally intended purpose?
- Is the collected or accessed information derived from activities protected under the First Amendment?
- Did the responsible parties conduct a PIA?
- Is the dissemination of intelligence products derived from personal information limited?
- Is the access to personal information restricted?
- Is the program subject to Executive oversight?
- Is the program subject to Congressional oversight?
- Is the program subject to Judicial oversight?
- Do accountability mechanisms enable the auditing of access to and use of personal information?

- Is the information made anonymous?

In Chapter II, it became clear that the type, use, and protection of U.S. persons' information contribute to a program's privacy costs.

Chapter III addressed a more fundamental issue: to determine where Americans have a legitimate privacy interest against which to assess privacy costs. The chapter argued that the 1970s interpretations of privacy are outdated. It demonstrated this by detailing the evolution of routine societal behaviors in the digital era, the increase in the number of parties that participate in standard social interactions, how there is more information being generated in modern times, and how that information is becoming extremely detailed and personal. This thesis accepts the twofold subjective and reasonable expectations of privacy established in Katz, but argues that contemporary society requires new interpretations of these standards in order to maintain the same level of privacy intended by the framers of the Constitution. Chapter III concluded that a person exhibits a subjective expectation of privacy by deliberately limiting the value and quantity of the objects, activities, or statements he or she shares with others and by restricting the number of people with whom he or she shares these things. Second, a reasonable expectation of privacy includes the pervasiveness of technology in society, particularly in regards to conducting routine social behaviors, surreptitious collection of personal information, and the level of detail in business records. That is, society is not willing to concede privacy interests despite the seeming erosion of personal privacy. In a free and open society, it is reasonable to expect that information shared with a company or another individual will not be shared with the government. After all, that is the intent of Fourth Amendment privacy protections.

Chapter IV transforms the lessons in Chapter II and III into a model for measuring privacy costs. The model comprises two types of assessments. First is the primary assessment, which focuses on establishing whether or not certain privacy concerns apply to an intelligence program and whether safeguards are in place to minimize—but not negate—those privacy concerns. Second, the comprehensive assessment identifies the overall privacy concerns, shortfalls in privacy safeguards, and what part of the program has the most negative effect on privacy costs. The comprehensive assessment also applies

a subjective review of the program's acceptability. While recognizing that public opinion is not an absolute determinant for what an intelligence program ought to do or avoid, it can nonetheless be a useful data point on the public's subjective tolerance of a particular intelligence program or practice. The template for this model is in Figure 8 and examples are in Figures 11 and 12.

Chapter V measured the privacy costs of the NSA BR metadata program according to the model. The analysis was revealing. While the public discourse since June 2013 until the reforms in January 2014 alluded to unacceptably high privacy costs, the alternative turned out to be true. The NSA program invoked few of the privacy concerns and had markedly effective and overlapping privacy safeguards. Moreover, while collection was unquestionably extensive, the telephone information used and passed to the FBI for investigative purposes affected a mere 0.00026 percent of the people whose information was collected by the program. As it turned out, the factor with the most negative effect on privacy costs was the absence of a PIA. Consequently, there have been compliance issues in the NSA program caused by technological and human errors that potentially could have been avoided. To minimize the privacy costs of the NSA BR program, the government would need to give adequate attention to this factor. Upon review of the 2014 intelligence reforms, there is no indication that one will be conducted. Additionally, the Chapter V analysis revealed that the reforms will produce no substantive improvements to the privacy costs of the BR metadata program. The reforms attempted to balance security and liberty by keeping a necessary program while altering some of the privacy practices. In the end, however, the balance essentially remained the same. The experience of the NSA program illuminates the futility of balancing security and liberty with one side of the scale empty.

B. IMPLICATIONS

With a method for measuring privacy costs now established, many ongoing domestic intelligence programs that affect Americans' privacy require a re-striking of the balance between security and liberty. The FBI's Terrorist Watch List is one example. As

of 2011, the list included 420,000 individuals.[240] To place someone on the list usually requires a preliminary terrorism investigation, but there are exceptions to this minimum standard.[241] This implies that the government can place Americans on the list for reasons other than a demonstrable connection to terrorism. Additionally, the government is supposed to remove a person from the Terrorist Watch List if there is insufficient justification for keeping him or her on the list, or if there is no active terrorism investigation on that person.[242] An IG report revealed that the average time it took the FBI to remove a name off the list was 1,112 days.[243] This implies that there could be Americans on the Terrorist Watch List that are not supposed to be, and whose privacy is being violated as a result. On the other hand, the Terrorist Identities Datamart Environment (TIDE) database had an increase in the total number of terrorist identifiers between 2011 and 2012 while having a simultaneous decrease in the number of Americans in that database.[244] Since the NCTC uses TIDE to nominate people to the Terrorist Watch List, the decrease of Americans in the database could indicate an increase in privacy protections for Americans in TIDE and, by extension, the watch list. The FBI also has a redress procedure through which a person can challenge his or her inclusion on the watch list;[245] however, this mitigates concerns only in so far it potentially corrects the government's infringement on that specific person's privacy.

---

240 "Terrorist Screening Center," Ten Years After: The FBI Since 9/11, FBI, September 2011, http://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/terrorist-screening-center.

241 U.S. Department of Justice, Office of the Inspector General, Audit Division, *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices*, Audit Report 09-25, May 2009, ii.,55.

242 Ibid., ii.,55.

243 Ibid., 55.

244 *Sharing and Analyzing Information to Prevent Terrorism: Hearing Before the House Committee on the Judiciary*, 111th Cong. (March 24, 2010) (statement of Timothy J. Healy, Director, Terrorist Screening Center, Federal Bureau of Investigation); ODNI, National Counterterrorism Center (NCTC), *TIDE Fact Sheet*, accessed February 28, 2014 and July 16, 2013, http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf.

245 *Five Years after the Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel: Hearing Before Senate Committee on Homeland Security and Governmental Affairs*, 111th Cong. (December 9, 2009) (statement of Timothy J. Healy, Director, Terrorist Screening Center, Federal Bureau of Investigation).

Notably, the FBI has improved on the issues addressed by the IG report.[246] These changes will not necessarily make the privacy costs tolerable. To determine the adequacy of the balance between security and liberty of the Terrorist Watch List requires an overall analysis of the privacy costs. Perhaps measuring these costs will identify areas for reform or perhaps the costs will be accepted for what they are. Either way, we cannot say that its security interest is accurately balanced against the privacy costs until that happens.

Similar to the NSA BR metadata program, the National Security Letters (NSLs) and the FISA 702 programs were also targets of the 2014 intelligence reforms.[247] Whether those changes will substantively mitigate privacy concerns requires a full understanding of the privacy costs. Will allowing companies to provide information about how many times they receive NSLs nullify the privacy concerns that exist? Is protecting incidental collection of U.S. person information that occurs in the FISA 702 program worth a possible decrease in intelligence efficiency? In the end, the presence of privacy costs does not always necessitate reforms. Changes that significantly affect how a program operates or that potentially decrease its effectiveness in the name of privacy concerns are not always desirable. Part of the nature of costs is what we are willing to give up in one area in order to gain in another. It is about the tough decision society must make: are the losses here worth the gains elsewhere? Sometimes the privacy costs will simply capture what the balance requires; it will reflect what privacy infringements must occur through an intelligence program in order to benefit security. Indeed, that is the debate to have and with a way to measure privacy costs, that is where this conversation goes next.

C. CONCLUDING REMARKS

Although this thesis argues for how best to account for privacy costs, which includes scrutinizing intelligence programs, it is not an argument for privacy over security. Making an argument for what privacy considerations must be taken into account

---

[246] U.S. Department of Justice, Office of the Attorney General, *Performance and Accountability Report*, Appendix C: Office of the Inspector General (IG) Follow-Up Audit of the DOJ Internal Controls over Reporting of Terrorism-Related Statistics, 2012, C1–C2.

[247] Office of the Press Secretary, "FACT SHEET."

is not to deny that the government might have a valid need to infringe on privacy-protected areas. It is simply to get to the end state: these are the privacy costs of carrying out the intelligence program.

The legitimacy of an intelligence program is inherently tied to how well it upholds Constitutional values while pursuing security threats. This occurs through striking the right balance between security and liberty. Measuring the privacy costs of a program is the requisite first step in reforming a program to decrease unnecessary costs, and the final step before posing the question to society of whether the overall privacy cost is worth the security benefit it promises.

LIST OF REFERENCES

Acxiom. "Who Are you?" Accessed March 1, 2014. https://aboutthedata.com/portal.

Bergen, Peter, David Sterman, Emily Schneider, and Bailey Cahall. "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New America Foundation, January 2014. http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0_0.pdf.

Berkowitz, Bruce. "Policies and Procedures for Protecting Security and Liberty." In *Protecting What Matters: Technology, Security, and Liberty since 9/11*, edited by Clayton Northouse, 74–87. Washington, DC: Brookings, 2005.

Bluekai. *Little Blue Book: A Buyer's Guide*. February 2014. http://bluekai.com/bluebook/bluekai-little-blue-book.pdf.

———. "Partner Program." Accessed March 1, 2014. http://bluekai.com/customers.php.

Brightcove. "Technology Partners." Accessed March 1, 2014. http://www.brightcove.com/en/partners/technology-partners.

Burger, Timothy J. "A Terror Tracking System by Any Other Name." *TIME*, May 14, 2003. http://content.time.com/time/nation/article/0,8599,451925,00.html.

Center for the Digital Future. *The 2013 Digital Future Report: Surveying the Digital Future*. Los Angeles, CA: University of Southern California, 2013. http://www.worldinternetproject.net/_files/_Published/_oldis/713_2013_digital_future_report_usa.pdf.

Cohen, David B. and John W. Wells, eds. *American National Security and Civil Liberties in an Era of Terrorism*. New York: Palgrave Macmillan, 2004.

Defense Advanced Research Agency (DARPA). *Report to Congress Regarding the Terrorism Information Awareness Program*. May 20, 2003.

———. "TIA Categories." Last updated November 25, 2002. http://www.darpa.mil/iao/TIASystems.htm. Site discontinued (screenshot is available at http://epic.org/events/tia_briefing/tia_categories.gif).

———. "Total Information Awareness (TIA) System)." Last updated November 25, 2002. http://www.darpa.mil/iao/TIASystems.htm. Site discontinued (screenshot is available at http://epic.org/events/tia_briefing/tia_screenshot.gif).

Delawala, Imtiyaz. "Intelligence Committee Leaders Defend NSA Surveillance." *ABC News*, June 9, 2013. http://abcnews.go.com/blogs/politics/2013/06/intelligence-committee-leaders-defend-nsa-surveillance/.

Doherty, Carroll. "Balancing Act: National Security and Civil Liberties in Post-9/11 Era." Pew Research Center, June 7, 2013. http://www.pewresearch.org/fact-tank/2013/06/07/balancing-act-national-security-and-civil-liberties-in-post-911-era/.

The Fact Checker (blog), http://www.washingtonpost.com/blogs/fact-checker/post/obamas-claim-that-every-member-of-congress-was-briefed-on-telephone-surveillance/2013/06/10/fd03ea8e-d21f-11e2-8cbe-1bcbee06f8f8_blog.html.

Federal Bureau of Investigation. "Ten Years After: The FBI Since 9/11: Terrorist Screening Center." Last modified September 2011. http://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/terrorist-screening-center.

Federation of American Scientists. "The Evolution of the U.S. Intelligence Community-An Historical Overview." Accessed March 2, 2014. http://www.fas.org/irp/offdocs/int022.html.

Foresee. "Partners." Accessed March 1, 2014. http://www.foresee.com/company/partners.shtml.

Fox, Susannah. "Pew Internet: Health." Pew Research Center. December 16, 2013. http://www.pewinternet.org/Commentary/2011/November/Pew-Internet-Health.aspx.

Gorman, Siobhan. "NSA Collects 20% or Less of U.S. Call Data." *Wall Street Journal*, February 7, 2014. http://online.wsj.com/news/articles/SB10001424052702304680904579368831632834004.

Hatch, Garrett. *Privacy and Civil Liberties Oversight Board: New Independent Agency Status*. CRS Report RL34385. Washington, DC: Library of Congress. Congressional Research Service, August 27, 2012.

Healy, Gene. "Beware of Total Information Awareness." *CATO*, January 20, 2003. http://www.cato.org/publications/commentary/beware-total-information-awareness.

Henry, Patrick. "A Chronology of U.S. Historical Documents: Give Me Liberty or Give Me Death." University of Oklahoma. Accessed September 16, 2013. http://www.law.ou.edu/ushistory/henry.shtml.

Johnson, Loch K. and James J. Wirtz. *Intelligence and National Security: The Secret World of Spies*, edited by Lock K. Johnson and James J. Wirtz. 2nd ed. New York: Oxford University, 2008.

Johnson, Thomas R. *Book III: Retrenchment and Reform, 1972-1980*. Volume 5, *NSA Period: 1952-Present* of a series on American Cryptography during the Cold War, 1945–1989. National Security Agency, 1998.

Kravets, David. "Which Telecoms Store Your Data the Longest? Secret Memo Tells All." *Wired*, September 28, 2011. http://www.wired.com/threatlevel/2011/09/cellular-customer-data/.

Litt, Robert S. *Privacy, Technology and National Security: An Overview of Intelligence Collection*. Office of the Director of National Intelligence. July 19, 2013. http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection?tmpl=component&format=pdf.

Louie, Gilman and Gayle von Eckartsberg. "Security and Liberty: How Technology Can Bridge the Divide." In *Protecting What Matters: Technology, Security, and Liberty since 9/11*, edited by Clayton Northouse, 63–73. Washington, DC: Brookings, 2005.

Markoff, John. "Pentagon Plans a Computer System that Would Peek at Personal Data of Americans." *New York Times*, November 9, 2002. http://www.nytimes.com/2002/11/09/politics/09COMP.html.

Massachusetts Institute of Technology. "Immersion: A People-Centric View of Your Email Life." Accessed March 1, 2014. https://immersion.media.mit.edu.

———. "Will Hunting" [Demo]." Accessed March 1, 2014. https://immersion.media.mit.edu/demo.

mobiThinking. "Global Mobile Statistics 2013 Part A: Mobile Subscribers; Handset Market Share; Mobile Operators." June 2013. http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#uniquesubscribers.

Mueller, John and Mark G. Stewart. "Hardly Existential: Thinking Rationally About Terrorism." *Foreign Affairs*, April 2, 2010. http://www.foreignaffairs.com/articles/66186/john-mueller-and-mark-g-stewart/hardly-existential.

Nakashima, Ellen. "NSA Is Collecting Less than 30 Percent of U.S. Call Data, Officials Say." *Washington Post*. Accessed March 5, 2014. http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington, DC: Government Printing Office, 2004.

———. *U.S. Signals Intelligence Directive 18: Legal Compliance and Minimization Procedures*. Revised January 25, 2011.

National Counterterrorism Center. *TIDE Fact Sheet*. Accessed February 28, 2014 and July 16, 2013. http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf.

Northouse, Clayton. "Providing Security and Protecting Liberty." In *Protecting What Matters: Technology, Security, and Liberty since 9/11*, edited by Clayton Northouse, 3–18. Washington, DC: Brookings, 2005.

Obama, Barrack. *Presidential Policy Directive-28*: *Signals Intelligence Activities*. January 17, 2014.

Office of the Director of National Intelligence. "DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001." News release, December 21, 2013. http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/991-dni-announces-the-declassification-of-the-exisitence-of-collection-activities-authorized-by-president-george-w-bush-shortly-after-the-attacks-of-september-11,-2001.

———. "DNI Clapper Declassified Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)." News release, September 10, 2013. http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document.

———. *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. June 8, 2013. http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/871-facts-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act

Olson, Parmy. "U.S. Senators: NSA Cellphone Spying Has Gone On 'For Years.'" *Forbes*, June 6, 2013. http://www.forbes.com/sites/parmyolson/2013/06/06/u-s-senators-nsa-cellphone-spying-has-gone-on-for-years/.

Peterson, Kristina and Siobhan Hughes. "Disclosures on NSA's Surveillance Embolden Its Critics in Congress." *Wall Street Journal*, August 24, 2013. http://online.wsj.com/article/SB10001424127887323665504579029362415300556.html.

Pew Research Center. "Internet User Demographics." Accessed February 8, 2014. http://www.pewinternet.org/data-trend/internet-use/latest-stats/.

———. "Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic." June 10, 2013. http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/.

———. "Mobile Technology Fact Sheet." December 27, 2013. http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.

———. "Trend Data (Adults)." Accessed February 8, 2014. http://www.pewinternet.org/Trend-Data-(Adults)/Online-Activites-Total.aspx.

Posner, Richard A. *Not a Suicide Pact: The Constitution in a Time of National Emergency*. New York: Oxford University, 2006.

The President's Review Group on Intelligence and Communications Technologies. *Liberty and Security in a Changing World*. December 12, 2013.

Privacy Rights Clearinghouse. "Fact Sheet 2b: Privacy in the Age of the Smartphone." Accessed September 13, 2013. https://www.privacyrights.org/fs/fs2b-cellprivacy.htm.

Richards, Julian. "Intelligence Dilemma? Contemporary Counter-terrorism in a Liberal Democracy." *Intelligence and National Security* 27, no. 5 (2012): 761-780.

Rosati, Jerel A. "At Odds with One Another: The Tension Between Civil Liberties and National Security in Twentieth-Century America." In *American National Security and Civil Liberties in an Era of Terrorism*, edited by David. B. Cohen and John W. Wells, 9–28. New York: Palgrave Macmillan, 2004.

Rosen, Jeffrey. "Total Information Awareness." *New York Times*, December 15, 2002. http://www.nytimes.com/2002/12/15/magazine/15TOTA.html.

Santayana, George. "History Repeated: The Dangers of Domestic Spying by Federal Law Enforcement." American Civil Liberties Union. Accessed September 12, 2013. https://www.aclu.org/sites/default/files/images/asset_upload_file893_29902.pdf.

Schneier, Bruce. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. New York: Copernicus, 2003.

Solove, Daniel J. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven, CT: Yale University, 2011.

Tabrizi, Susan J. "At What Price? Security, Civil Liberties, and Public Opinion in the Age of Terrorism." In *American National Security and Civil Liberties in an Era*

of Terrorism, edited by David. B. Cohen and John W. Wells, 185-201. New York: Palgrave Macmillan, 2004.

Treverton, Gregory F. *Intelligence for an Age of Terror*. Cambridge: Cambridge University, 2009.

U.S. Department of Commerce. Bureau of the Census. *National Population Projections, 2008*. Washington, DC: Government Printing Office, 2012. Table 2.

———. *Population Estimates: Annual Resident Population Estimates of the United States by Age and Sex.* Washington, DC: Government Printing Office, 2002.

———. *Statistical Abstract of the United States, 2012*. Washington, DC: Government Printing Office, 2012. Table 1188.

U.S. Department of Defense. Office of the Inspector General. *Terrorism Information Awareness Program*. D-2004-033. December 12, 2003.

U.S. Department of Justice (DOJ). Office of Intelligence. National Security Division. *The Attorney General's Annual Report on Access to Certain Business Records for Foreign Intelligence Purposes under the Foreign Intelligence Surveillance Act*. April 2012.

———. *The Attorney General's Annual Report on Access to Certain Business Records for Foreign Intelligence Purposes under the Foreign Intelligence Surveillance Act*. April 2011.

———. *Memorandum of the United States in Response to the Court's Order Dated January 28, 2009*. Docket Number: BR 08-13. February 17, 2009.

———. *Report of the United States*. Docket Number: BR 09-09. August 17, 2009.

———. *Report on the National Security Agency's Bulk Collection Programs Affected by USA PATRIOT Reauthorization*. February 2, 2011.

———. *Report on the National Security Agency's Bulk Collection Programs Affected by USA PATRIOT Reauthorization*. December 14, 2009.

U.S. Department of Justice. Office of the Attorney General. *Performance and Accountability Report*. Appendix C: Office of the Inspector General Follow-Up Audit of the DOJ Internal Controls over Reporting of Terrorism-Related Statistics. 2012.

U.S. Department of Justice. Office of the Inspector General. Audit Division. *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices*. Audit Report 09-25. May 2009.

U.S. Senate. "Church Committee Created." Accessed March 2, 2014. http://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm.

U.S. Senate. Committee on Commerce, Science, and Transportation. Office of Oversight and Investigations. *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*. December 18, 2013.

U.S. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. *Intelligence Activities and the Rights of Americans: Final Report*. Book II, Senate Report No. 94-755. 1976.

Westin, Alan F. "How the Public Sees the Security-versus-Liberty Debate." In *Protecting What Matters: Technology, Security, and Liberty since 9/11*, edited by Clayton Northouse, 19–36. Washington, DC: Brookings, 2005.

White House. Office of the Press Secretary. "FACT SHEET: Review of U.S. Signals Intelligence." News release, January 17, 2014. http://www.whitehouse.gov/the-press-office/2014/01/17/fact-sheet-review-us-signals-intelligence.

———. "Remarks by the President on Review of Signals Intelligence." News release, January 17, 2014. http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

WolframAlpha. "Personal Analytics for Facebook." Accessed March 1, 2014. http://www.wolframalpha.com/facebook/.

Wyden, Ron. "Wyden Calls for Congressional Oversight, Accountability of Total Information Awareness Office." News release, January 15, 2003. http://www.wyden.senate.gov/news/press-releases.

Zengerle, Patricia. "FBI Official Says NSA Programs Helped Foil NYSE Bombing Plot." *Reuters*, June 18, 2013. http://www.reuters.com/article/2013/06/18/us-usa-security-nyse-idUSBRE95H0QT20130618.

Zengerle, Patricia and Tabassum Zakaria, "NSA Head, Lawmakers Defend Surveillance Programs." *Reuters*, June 18, 2013. http://www.reuters.com/article/2013/06/18/us-usa-security-idUSBRE95H15O20130618.

Zuckerman, Jessica. "Fifty-Third Terror Plot Foiled Since 9/11: Bombing Targets U.S. Financial Hub." Heritage Foundation, Issue Brief 3758. 2012. http://thf_media.s3.amazonaws.com/2012/pdf/ib3758.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California